МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ЧЕРКАСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОГДАНА ХМЕЛЬНИЦЬКОГО**

ОРГАНІЗАЦІЙНО-ЕКОНОМІЧНИЙ МЕХАНІЗМ ПРОТИДІЇ ЗЛОЧИНАМ В ЕКОНОМІЧНІЙ СФЕРІ

***Колективна монографія за редакцією
Черевка О.В., Мігус І.П., Гнилицької Л.В.***

Черкаси – 2016

УДК 330 (477) : 343.53 (477)
ББК 65.9 (4 укр) – 983+67.408.122 (4 укр)
Ч 46

Рекомендовано до друку радою Черкаського національного університету імені Богдана Хмельницького (Протокол № 3 від 28 листопада 2016 р.)

Рецензенти:

Шпильова В.О. - доктор економічних наук, професор, Черкаська філія ПВНЗ «Європейський університет»

Прямухіна Н.В. - доктор економічних наук, професор, Черкаський державний технологічний університет

ISBN 978-966-920-166-9

Ч 46 Організаційно-економічний механізм протидії злочинам в економічній сфері : монографія / За ред. Черевка О.В., Мігус І.П., Гнилицька Л.В. – Черкаси : видавець Чабаненко Ю.А. – Черкаси, 2016. – 466 с.

У монографії розкривається сутність та види злочинів в економічній сфері, які здійснюються різноманітними суб'єктами на макро та мікро рівнях. Приділено увагу вивченню механізмів протидії злочинам в економічній сфері. Встановлено роль кадрової безпеки у реалізації механізму протидії економчим злочинам. Досліджено інформаційне забезпечення механізму протидії злочинам в економічній сфері. Вивчено контрольно-аналітичні технології управління ризиками корпоративного шахрайства в системі економічної безпеки суб'єктів господарювання. Запропоновано основні напрями вдосконалення організаційно-економічного механізму протидії злочинам в економічній сфері.

Розраховано на науковців, фахівців з питань тіньової економіки та економічної безпеки, студентів економічних спеціальностей та інших зацікавлених осіб.

УДК 330 (477) : 343.53 (477)
ББК 65.9 (4 укр) – 983+67.408.122 (4 укр)
Ч 46

ISBN 978-966-920-166-9

© Черевко О.В., Мігус І.П., Гнилицька Л.В., 2016
© Черкаський національний університет імені Богдана Хмельницького, 2016

ЗМІСТ

ПЕРЕДМОВА 5

РОЗДІЛ 1. СИСТЕМНИЙ ПІДХІД ДО ВИВЧЕННЯ ЗЛОЧИНІВ В ЕКОНОМІЧНІЙ СФЕРІ: ОСНОВНІ ЕТАПИ РОЗВИТКУ 8

1.1. Злочини у економічній сфері, що становлять загрозу економічній безпеці фінансових установ, та напрями протидії їм 9

1.2. Рейдерство як один із видів економічних злочинів 29

1.3. Концептуальні основи системи економічної безпеки 55

1.4. The Comparison of Economic Crime Level in Selected European Countries Using The Zero Unitarization Method 75

1.5. Конкурентна розвідка та контррозвідувальна діяльність як функції системи економічної безпеки підприємства 96

1.6. Банківські кризи, як передумова виникнення економічних злочинів у банківській сфері 106

РОЗДІЛ 2. МЕХАНІЗМИ ПРОТИДІЇ ЗЛОЧИНАМ В ЕКОНОМІЧНІЙ СФЕРІ 134

2.1. Напрями удосконалення системи економічної безпеки будівельних підприємств для запобігання злочинам у економічній сфері 135

2.2. Концептуальний підхід до вдосконалення державного моніторингу корупційних загроз на систему економічної безпеки державними регуляторами 153

2.3. Механізм забезпечення економічної безпеки службами безпеки охоронних підприємств 171

2.4. Організація системи фінансового моніторингу в комерційних банках 199

РОЗДІЛ 3. РОЛЬ КАДРОВОЇ БЕЗПЕКИ У РЕАЛІЗАЦІЇ МЕХАНІЗМУ ПРОТИДІЇ ЕКОНОМІЧНИМ ЗЛОЧИНАМ 224

3.1. Організація незалежного зовнішнього аудиту підсистеми організації безпеки праці на будівельних підприємствах з позицій економічної безпеки 225

3.2. Практичні аспекти забезпечення кадрової безпеки на підприємствах 238

3.3. Концептуальний підхід до оцінки рівня ділової репутації банку в системі економічної безпеки банку 262

3.4. Ефективна реалізація інтелектуально – трудового потенціалу як рушійна сила інноваційного розвитку та безпеки національної економіки 283

3.5. Роль верифікації в протидії злочинам в соціальній сфері та загрозам соціальній безпеці 302

РОЗДІЛ 4. ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ МЕХАНІЗМУ ПРОТИДІЇ ЗЛОЧИНАМ У ЕКОНОМІЧНІЙ СФЕРІ 324

4.1. Правове та інформаційне забезпечення захисту комерційної й банківської таємниці як складова економічної безпеки фінансових установ 325

4.2. Організація інформаційної безпеки банківських установ в системі економічної безпеки 347

4.3. Державна політика щодо забезпечення інформаційної безпеки 366

4.4. Адміністративно-правові концепти корпоративних моделей інформаційної безпеки підприємств 389

4.5. Security of electronic banking in Poland 413

РОЗДІЛ 5. КОНТРОЛЬНО-АНАЛІТИЧНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ РИЗИКАМИ КОРПОРАТИВНОГО ШАХРАЙСТВА В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ 434

5.1. Антикорупційний аудит як інструмент протидії корупції та хабарництву у діяльності суб'єктів господарювання 435

5.2. Економічна природа шахрайства з фінансовою звітністю та способи його подолання 441

5.3. Маніпулювання обліковими даними як складова професійного ризику бухгалтера 454

ПЕРЕДМОВА

Сучасний період економічного розвитку характеризується погіршенням ситуації в сфері економічної діяльності, яке пов'язане з економічною кризою, що вразила не тільки нашу країну, але і всю світову економіку. В умовах економічної кризивідбувається зростання рівня злочинності, зокрема, у економічній сфері. Небезпека злочинності в сфері економічної діяльності полягає не тільки в заподіянні матеріальних збитків державі, суспільству і громадянам, а й у здатності до дестабілізації економічної системи в цілому. Її масштаби на разі такі, що впливають на всі сторони життя суспільства. Протиріччя, що виникають між загальноприйнятими, встановленими правом і цивілізованими формами і методами господарської діяльності та незаконними способами збагачення призводять до безладів, прояву невдоволення, протестів і мітингів. Якщо своєчасно не усувати ці протиріччя, в суспільстві відбувається утворення і відтворення паралельних цілісних соціально-економічних структур протиправної орієнтації, здатних при збереженні існуючих тенденцій підпорядкувати собі всі ресурси країни.

З огляду на це, нові економічні умови, ринкові тенденції, що формуються в сучасних соціально-політичних обставинах, вимагають продуманих заходів щодо забезпечення безпеки в економічній діяльності, стимулювання сумлінного підприємництва –як гарантії майбутньої економічної стабільності суспільства, а отже, і його політичного життя, і духовної сфери.

Розвиваючи власну економічну систему, будь-яка країнастикається з проблемою злочинності в сфері економіки.Протидія злочинам подібного роду є однією з важливих задач, тому що злочини в економічній сфері можуть підривати економічні основи держави, сприяти створенню тіньового ринку, розвитку корупційних зв'язків і, якнаслідок, призводити до ослаблення економічної могутності країни.

Під економічними злочинами прийнято розуміти суспільно небезпечні діяння, які передбачають посягання на фінансово-економічні відносини, що

забезпечують процес виробництва / реалізації / споживання різних товарів і послуг. Велика частина злочинів у сфері економіки вчиняється з метою підриву діяльності тієї або іншої компанії і отримання фінансової наживи.

Економічні злочини завдають істотної шкоди як окремим громадянам і організаціям, так і безпосередньо державі в цілому. Найчастіше вчинення таких злочинівпов'язане з втратою об'єктів нерухомого майна, неотриманням або недоотриманнямприбутку, якийкраїна могла б і повинна булаотримати від використання протиправно вилученого у неї майна, а також несплатою податків і зборів, розкраданням бюджетних коштів.

Злочини в економічній сфері, зокрема легалізація (відмивання) доходів,одержаних злочинним шляхом, рейдерство, хабарництво та інші корупційні та посадові злочини, пов'язані з нецільовим використанням бюджетних коштів, злочини у сфері державного оборонного замовлення, житлово-комунального комплексу, сплати податків і зборів, охорони здоров'я та освіти, пов'язані з приватизацією державногомайна і реалізацією державних непрофільних активів, належать до числа найбільш небезпечних загроз для економічної безпеки держави.

Високий рівень злочинів в економічній сфері не дозволяє забезпечити необхідний рівень економічного зростання, ускладнює реформування економіки, чинить негативний вплив на торговельну тазовнішньоекономічну діяльність України, перешкоджає можливості вдосконалення бюджетної, податкової, страхової іінших сфер фінансової системи нашої держави.

У сучасних умовах політичної та економічної нестабільності на державному рівні постає необхідність прицільно сконцентрувати зусилля на механізмах протидії економічним злочинам, нейтралізуватитакі явища, як маніпулювання ринком, незаконний обороті використання інсайдерської інформації, картельні змови,рейдерство та інші злочини, що посягають на основу економічногоукладу –приватну власність, та такі, що пов'язані із ухиленням від сплати податків та іншихплатежів до бюджету.

Боротьба зі злочинністю у сфері економічної діяльності не тільки є необхідною умовою для здійснення глибоких економічних перетворень, а й визначає подальшу долю України. Боротьба з економічними злочинами була і залишається однією із найбільш гострих проблем у нашій країні, оскільки саме ці види злочинів завдають величезної майнової шкоди державі та порушують конституційні права людини і громадянина.

Залучення до відповідальності винних у вчиненні економічних злочинів осіб та структур, оцінювання та відшкодування завданих державі матеріальних збитків – найважливішізавдання, що стоять перед органами влади, до функцій яких належить забезпечення національної безпеки України. Однак велика кількість питань, що стосуються державно-правового механізму боротьби з економічною злочинністю, все ще залишаються недостатньо опрацьованими, а засоби і методи боротьби з економічними злочинами– недостатньо ефективними. Тому беззаперечною на сьогодні є велика практична значимість і необхідність проведення комплексного наукового аналізу та дослідження механізмівборотьби з економічною злочинністю як важливого напряму процесу забезпеченняекономічної та національної безпеки держави.

З повагою,
ректор Черкаського національного університету
імені Богдана Хмельницького,
професор кафедри менеджменту та економічної безпеки,
професор, д.е.н. ***Черевко Олександр Володимирович***

завідувач кафедри менеджменту та економічної безпеки
Черкаського національного університету
імені Богдана Хмельницького,
професор, д.е.н. ***Мігус Ірина Петрівна***

професор кафедри обліку підприємницької діяльності
ДВНЗ «Київський національний економічний університет
імені Вадима Гетьмана»,
професор, д.е.н. ***Гнилицька Лариса Володимирівна***

РОЗДІЛ 1
СИСТЕМНИЙ ПІДХІД ДО ВИВЧЕННЯ ЗЛОЧИНІВ В ЕКОНОМІЧНІЙ СФЕРІ: ОСНОВНІ ЕТАПИ РОЗВИТКУ

1.1. ЗЛОЧИНИ У ЕКОНОМІЧНІЙ СФЕРІ, ЩО СТАНОВЛЯТЬ ЗАГРОЗУ ЕКОНОМІЧНІЙ БЕЗПЕЦІ ФІНАНСОВИХ УСТАНОВ, ТА НАПРЯМИ ПРОТИДІЇ ЇМ

МІГУС ІРИНА ПЕТРІВНА, *д.е.н., професор,*
завідувач кафедри менеджменту та економічної безпеки,
ЗАЧОСОВА НАТАЛІЯ ВОЛОДИМИРІВНА*, к.е.н., доцент,*
доцент кафедри менеджменту та економічної безпеки
Черкаський національний університет імені Богдана Хмельницького

Економічні злочини характеризуються як злочини «білих комірців», і є одними із найпідступніших і найменш помітних широкому загалу. Суб'єкти господарювання, проти яких було вчинено злочинні дії, у ряді випадків навіть не звертаються по допомогу до силових структур, оскільки не бажають констатувати факт наявності вад та прорахунків у власних системах економічної безпеки, що не змогли забезпечити надійний рівень захисту їх корпоративних ресурсів від злочинних посягань. Таким чином, через недостатність інформації та її приховування,важко достовірно оцінити масштаби економічної злочинності та її наслідки для функціонування вітчизняного фінансового ринку та результатів діяльності його учасників.

Близьким по суті поняттям до поняття економічного злочину є категорія фінансового злочину. В широкому сенсі, фінансові злочини – це будь-які ненасильницькі злочини,що спричиняють/можуть спричинити фінансові втрати. Загалом, фінансові злочини – це злочини, які спрямовані проти фінансових інститутів (як державних, так і приватних) і вчинені з використанням фінансових систем та відносин, за допомогою фінансових документів. Найбільш яскравими прикладами фінансових злочинів є ухилення від сплати податків, шахрайство (шахрайство з платіжними картками, іпотечне шахрайство, корпоративне шахрайство, шахрайство з цінними паперами (включаючи інсайдерську торгівлю), банківське шахрайство тощо), хабарництво, розкрадання, крадіжка персональних даних, підробка грошей та легалізація доходів, отриманих злочинним шляхом [1].

Фінансові злочини – це ризики безпеки, які не можуть бути виміряні тільки в параметрах, що піддаються обчисленню. Вони призводять до таких негативних наслідків, як фінансова нестабільність і знижена продуктивність суб'єкта господарювання. Крім того, вони можуть виявитися причиною пильної уваги преси, що провокує негативну реакцію від партнерів, клієнтів та контрагентів і, як наслідок, призводить до втрати ділової репутації та зниження ринкової вартості компанії.

У більшості випадків фінансові злочини вчиняються із залученням фінансових установ, або направлені проти них.

Проблема розширення меж економічної та фінансової злочинності є характерною для сучасної економіки України. Стрімкими темпами збільшується не лише кількість економічних злочинів, але і ускладнюються та набувають нових форм види злочинних дій та механізми їх вчинення у економічній та фінансовій сферах.

Актуальність дослідження проблеми протидії економічним злочинам підтверджується численними науковими працями вітчизняних дослідників. Зокрема, Рогозін С. М. вивчає питання попередження економічної злочинності [2], конкретизує інформаційно-правові засади протидії економічній злочинності [3], Раєцька Л. В.розглядає необхідність протидії економічнійзлочинності як засобу забезпечення економічної безпеки держави[4], Кузьмін Р. Р. визначає основні напрями загально-соціального запобігання економічній злочинності в Україні [5];Пчеліна О. В. піднімає проблему використання підприємств у технологіях економічної злочинної діяльності [6], Ляшенко М. М. робить спроби встановити загальні причини скоєння економічних злочинів та виявити напрямки їх профілактики [7].Окремі питання щодо вчинення економічних злочинів, у тому числі у фінансовій сфері, знаходимо у роботах таких науковців, як Медвідь Т. А.[8], Степанюк Р. Л. [9], Вівчар О. І. [10], Погорелов О. В. [11], Гула Л. Ф. [12].Попри це, напрями протидії злочинам у економічній сфері, що становлять загрозу економічній безпеці фінансових установ, і досі потребують конкретизації та додаткового вивчення з огляду на постійну зміну

механізмів їх вчинення, розширення форм та видів і збільшення масштабів їх наслідків як для стану економічної безпеки окремих суб'єктів господарювання, так і для економічної системи держави в цілому.

Переважна більшість економічних злочинів скоюються із використанням механізмів фінансового посередництва. Оскільки кінцевою метою вчинення цього виду злочинних дій є отримання зловмисниками прибутку, або іншого економічного ефекту для задоволення особистих потреб, фінансові установи виявляються втягнутими у процеси виведення чи перерахунку грошових коштів задля подальшого їх використання на різні цілі. Водночас, фінансові установи можуть бути і об'єктом вчинення злочинів, зокрема у випадках шахрайських дій у банківській, кредитній, страховій сферах, на ринку Forex та ринку цінних паперів тощо.

У 2009 році компаніюPriceWaterhouseCoopers (PwC) було проведено Всесвітній огляд динаміки економічної злочинності та визначено, які економічні злочини були характерними для України у період кризи. Загалом, 45% суб'єктів господарювання виявилиекономічні злочини впродовж 2008 року; корупція та загроза звільненняв період кризи були виділенісеред основних факторів, щосприяли зростаннюекономічної злочинності; розкрадання майна іхабарництво були визначені якнайбільш поширені видиекономічної злочинності. Дослідження продемонструвало, що 40% респондентів не проводятьабо не чули про проведеннярозслідувань для виявленняшахрайських операцій на своїхсуб'єктах господарювання; 24% із виявлених економічнихзлочинів було ідентифіковановипадково та без використанняпідконтрольних керівництвуметодів; прогнози щодо майбутніхризиків шахрайства в Україні всередньому були вдвічі вищими упорівнянні з іншими країнами. Варто відзначити, що майже четверта частина усіх опитаних – 24,62% представляли фінансових сектор.

У 2008 році більше 50% всіх економічнихзлочинів в Україні, у порівнянні з26% у глобальному огляді, буловиявлено за допомогою процедуруправління ризиками, формальнихканалів інформування керівництвапро шахрайство або

внутрішньоїслужби безпеки. Таким чином, можна вести мову про досить високий, але все таки недостатній рівень організації систем економічної безпеки вітчизняних суб'єктів господарювання. 24% випадків шахрайства в Українібуло виявлено випадково упорівнянні з 16% у всьому світі. Цідані свідчать про те, що українськийбізнес все ще покладається «навипадок» при виявленні економічних злочинів.Лише 7% виявлених випадківшахрайства в Україні, у порівнянні з17% у глобальному вимірі, визначають задопомогою внутрішнього аудиту, щопідтверджує ранню стадію розвиткуцієї функції в нашій державі. Напрямами, у яких прогнозувалось зростання кількості випадків економічних злочинів, були наступні: корупція і хабарництво (50%), розкрадання майна (30%), порушення ІТ-безпеки (25%)[13, с.3-4].

Прогнози справдились. Коли у 2011 році PwC провела огляд економічної злочинності в світі повторно, кіберзлочинність стала одним із п'яти найпоширеніших економічних злочинів в Україні.Понад 25% суб'єктів господарювання не мають відповідних політик та механізмів реагування на кіберзлочини, розроблених у рамках функціонування їх систем економічної безпеки.46% опитаних не проходили навчання в області кібербезпеки, а 58% респондентів з України заявили, що в їхніх організаціях відсутній процес моніторингувідвідування соціальних мереж.36% респондентів в Українірозглядають кіберзлочинністьяк зовнішню загрозу економічній безпеці суб'єктів господарювання, 24% – як внутрішню загрозу, а 34%вважають, що загроза існує якззовні, так і всерединіорганізації. Серед підрозділів, які наражаютьорганізації на ризикикіберзлочинності, респонденти зазначили відділ фінансів(47%), відділ маркетингу тапродажів (37%), юридичнийвідділ (27%), підрозділивертикалі операційноїдіяльності (22%), а такожпредставників вищогокерівництва (29%). Подібнатенденція спостерігалася і вінших країнах.

Найменш ризиковими у даному контексті буливизнані відділ інформаційноїбезпеки та фізичної безпеки(16% опитаних), а також відділ зуправління персоналом (10%).При цьому не варто забуватипро те, що правопорушникамиможуть виявитисяспівробітники будь-якоговідділу.

Загалом, 36% організацій зафіксували випадки економічної злочинності у 2010 році, представники третини опитанихсуб'єктів господарюваннявизнали, що не проводять оцінку ризиків шахрайства, і при цьому кількість внутрішніх шахрайських операцій суттєво зросла (на 22%) у порівнянні з 2009 роком.Незаконне привласнення майна (73%), корупція та хабарництво (60%) залишились найпоширенішими видами економічної злочинності в Україні.40% злочинів були скоєні вищим керівництвом організацій, і кожен п'ятий працівник, який скоїв економічний злочин, не поніс належного покарання.

У підсумку можна відзначити, що з 50% усіх економічних злочинів, за даними опитування, респонденти стикнулись у секторі фінансових послуг, з 29% – у сфері страхування [14, с.5-11]. Типовий суб'єкт економічнихзлочинів в Україні – цечоловік із вищою освітою увіці 31-50 років, який працює на підприємстві, в установі, в організації 3-10 років.

Українськими організаціями було вжито таких заходів проти зовнішніх шахраїв: інформування правоохоронних органів (71%); подача цивільних позовів, включаючи вимоги про відшкодування збитків (64%); припинення ділових стосунків (57%); інформування відповідних органів нагляду (43%) [14, с.14].

У 2014 році найвищий відсоток економічної злочинності за даними PwC було зафіксовано у Південній Африці (69%). На другому місці за цим показником опинилась Україна – 63% проти 36% у 2011 році [15, с.47]. Такі дані свідчать про стрімке зростання масштабів економічної злочинності у нашій країні, та необхідність підвищення рівня організації та функціонування систем економічної безпеки вітчизняних суб'єктів господарювання, у тому числі і фінансових установ.

Щодо економічних злочинів, які стосуються фінансових посередників, нині, на початку 2016 року, можна виділити кілька найбільш значимих векторів злочинних дій проти них.

Зокрема, у банківському секторі, що є найбільшим сегментом фінансового ринку, поширеним видом економічного злочину є крадіжка даних про клієнтів

банків задля їх продажу зацікавленим особам або використання з метою заволодіння коштами. По причині розвитку сфери безготівкових розрахунків, досить часто для вчинення злочину використовуються пластикові картки. У переважній більшості випадків, зловмисником у таких видах злочинів виявляються співробітники банківських установ, що мають безпосередній доступ до усієї інформації про осіб, які обслуговуються у їх відділенні. Трапляються випадки, коли працівники банку для крадіжки грошей підшукують клієнтів, які мають на рахунках значні суми, але рідко користуються послугами банку, тому не одразу помітять зникнення частини коштів. Викрадені гроші можуть спочатку перераховуватися на карту сторонньої особи, а потім на рахунок картки зловмисника.

Також варто згадати випадки, коли менеджери банків, користуючись службовим становищем, оформлювали на клієнтів відділення банківської установикредитні карти без їх відома, а через деякий час переводили у готівку фінансові активи, що були доступними по цим карткам. Банківські співробітники можуть переводити кошти з каси на рахунки своїх близьких родичів або свої власні, а щоб приховати недостачу –недокладати гроші в касети банкоматів. Факт вчинення такого злочину можна виявити лише під час ревізії роботи банкоматів.

Крадіжки готівки з банківських установ часто трапляються при її перевезенні, причому винними у багатьох випадках бувають інкасатори. Маючи прямий доступ до грошових коштів, ці людинерідко піддаються спокусі та свідомо ідуть на вчинення злочину. Подібну природу мають злочини, пов’язані із крадіжкою валюти у пунктах обміну, що вчиняються особами, які обслуговують обмінні операції та мають доступ до валютних цінностей.

Вчинення економічних злочинів проти власної фінансової установи властиво не лише для менеджерів нижчої та середньої ланки. Відомі випадки, коли керівництво банківських установдавало дозвіл на видачу свідомо неповоротних і матеріально незабезпечених кредитів підконтрольним комерційним організаціям – так званим «технічним позичальникам», за

допомогою яких із банку виводились активи для подальшого використання зловмисниками. Також існують схеми, коли представники топ-менеджменту банківських установ через підставних осіб і під приводом фінансування філій банку проводили фіктивну передачу грошових коштів своїм спільникам і згодом розпоряджались отриманими сумами грошей на власний розсуд.

Існують і більш складні схеми вчинення економічних злочинів проти банківських установ. Так, відомою є тіньова фінансова схема з переведення в готівку і виведення капіталів за кордон під виглядом здійснення угод купівлі-продажу цінних паперів. У процесі її використання, готівкові кошти недобросовісні клієнти отримували за допомогою підставних фізичних осіб в банкоматах, касах брокерських компаній і банків. Зовні все виглядає так, ніби клієнт брокерської контори, погравши якийсь час на біржі, забирає свої гроші назад в готівковій формі.

Відомими є випадки, коли в банках, в яких діяла заборона на залучення депозитів, були в короткі терміни здійснені дії щодо масового відкриття рахунків фізичним особам і індивідуальним підприємцям, а також прийняття від них грошових вкладів. Згодом залучені кошти були викрадені зловмисниками під виглядом здійснення операцій із придбання цінних паперів, вартість яких була штучно завищена. Звісно, вчинити такий злочин не можливо без залучення до злочинних схем вищого керівництва банківської установи.

Найбільш поширеним випадком вчинення економічного злочину проти банку зі сторони його клієнтів є привласнення коштів через незаконне отримання кредитів по фальшивим або викраденим документам.

Але найбільшою загрозою для економічної безпеки банків та їх клієнтів є хакерські атаки. Ця проблема є характерною не лише для України.Так, у 2015 році збитки банківської системи Росії від дійкіберзлочинців склали близько 1 млрд.дол. США. Для кіберзлочиніців не існує меж і кордонів, тому цей вид економічної злочинності по праву може вважатися транснаціональним. Найпростішими прикладами злочинів, що вчиняються хакерами, може бути підключення послуг мобільного сервісу для проведення операцій на

банківському рахунку без відома його власника. Так хакер отримує доступ до коштів клієнта банку, і через телефон може знімати їх з рахунку без згоди клієнта. Більш складним варіантом вчинення подібного злочину є використання шкідливого програмного забезпечення для смартфонів на базі Android, що дозволяє зловмисникам в короткі терміни створювати ботнет з мобільних гаджетів для подальшої роботи з рахунками їх власників.

Фіксуються випадки вчинення злочинних дій проти банків, що відбуваються за наступною схемою. Злочинець отримує в банку неіменну картку, вносить на неї через банкомат готівку, а потім в тому ж банкоматі їх знімає і отримує чек про проведену операцію.Далі шахрай відправляє чек до свого спільника, який мав віддалений доступ до заражених вірусом POS-терміналів, що, як правило, перебувають за межами країни. Через термінали за кодом операції, зазначеної в чеку, спільник формує команду на відміну операції зі зняття готівки: на терміналі це виглядає, наприклад, як повернення товару. В результаті скасування операції баланс карти відновлюється миттєво, і у зловмисника залишаються видані готівкові кошти на руках і колишній баланс на картці. Злочинці повторюють ці дії до тих пір, поки в банкоматах не закінчується готівка.

Відомі випадки, коли для здійснення розкрадань коштів банків хакери створювали і реєстрували за всіма міжнародними стандартами власні платіжні системи. Це дає їм можливість здійснювати цільові атаки не тільки на процесингові центри окремо взятих банків, але і на світові системи обміну міжбанківськими фінансовими повідомленнями.

Прикладом найпростішого шахрайствау сфері страхування можуть слугувати випадки, коли застраховані особи одержують виплати пофакту фіктивного оформлення нещасних випадків, у тому числі шляхом виправлення дат настання страхових випадків; не існуючих, але медично грамотно оформлених «переломів», «розривів зв’язок» тощо. В таких випадках страховики отримують цілий «злочинний» набір: це й шахрайство, і зловживання посадовими повноваженнями, і підробка документів, і

хабарництво, і службова підробка. Однак, основу злочинних дій становить саме шахрайство шляхом імітації страхового випадку та спроби одержання страхового забезпечення за підробленими довідками про нещасний випадок [16].

Крім того, вчинення економічних злочинів проти страхових компаній можливо через спроби отримати страхові відшкодування по обманним деклараціям про пожежі, викрадення автомобілів, пограбування квартир тощо. Уокремих випадках сума страхового відшкодування завищена або оголошення страхової суми вище дійсної вартості об'єкта страхування. Злочином є багаторазове одночасне страхування об'єкта страхування відразу в декількох страхових компаніях, неповідомлення всіх обставин, що мають значення для визначення страхового ризику; пред'явлення завищених вимог про відшкодування шкоди, фальсифікація факту настання страхового випадку тощо.

Варіантами злочинних дій при майновому страхуванні є: підпал майна, затоплення суден, провокування аварій, фіктивне складання документів про заподіяні збитки від стихійних дій.

Розглянемо, які загрози супроводжують функціонування систем економічної безпеки вітчизняних ломбардів. Так, бувають випадки, коли речі, які є предметом застави в ломбарді, вилучаються в установленому законом порядку на тій підставі, що власником речі є інша особа. Тобто виїмки речей в ломбардах у кримінальних справах створюють особливу ситуацію, коли ломбард змушений нести невиправдані витрати по поверненню втрачених грошей, де зусилля керівництва установи нерідко є марними. А у деяких випадках речі у ломбардів вилучаються незаконно.Булизафіксовані випадки, коли нечесні співробітники поліції (свого часу міліції), використовуючи своє службовестановище для вирішення питання повернення речей істинним власникам (родичам або знайомим) без порушення кримінальної справи або взагалі без всяких процедур, а керівники ломбардів просто списували такі збитки.

Крім того, інтересам ломбардів, так само як і іншим фінансовим установам, загрожують злочинні дії персоналу, що може викрасти активи, які належать установі або її клієнтам, навмисно спотворювати інформацію про вартість заставного майна тощо.

Зважаючи на це, економічна безпека ломбарду для протидії таким випадкам, має бути заснована на трьох складових:

- технологічні заходи (відіофіксація угод, «чорний список», психологічні навички тощо);

- організаційні заходи (посадові інструкції, інформаційна активність з відділеннями ломбардів та контрагентамиломбардів, відстеження ситуації в місті і в іншихрегіонах тощо);

- юридичний захист інтересів ломбарду.

Найбільш важливою складовою економічної безпеки ломбардів є юридичний захист інтересів установи. Юридичний захист від втрат при проведенні виїмок полягає в тому, щоб всі процеси від початку до кінця відбувалися і проводилися в рамках закону. Щоб мінімізувати втрати, потрібно знати усі особливості дій правоохоронних органів у випадку проведення виїмок, правила взаємин із ними, права ломбарду щодо задоволення вимог до позичальника тощо.

Юридичний захист в ломбарді від втрат при проведенні виїмок речей можна розділити на два етапи: на процедуру виїмки і дії щодо компенсації витрат, пов’язанихіз можливою втратою грошей у вигляді суми позики і відсотків.

Для вітчизняних кредитних спілок також є характерними деякі види економічних злочинів. Більшість із них ініціюються керівниками або власниками спілок чи їх персоналом. Можна навести такий приклад: пайовики вносять гроші в кредитну спілку, директор видає кредити членам союзу, які ці кредити не погашають.Поширеними є випадки видачі персоналом спілок позик своїм друзям і знайомим по процентній ставці, що є нижчою середньої ставки залучення заощаджень. При цьому позиками за найнижчою ставкою успішно

користуються пов’язані із керівниками або персоналом спілки особи, а також їх колеги. Для інших учасників процентна ставка буде надзвичайно високою, що призводитиме до втрати наявних та потенційних клієнтів.Впродовж певного періоду часу гроші вкладникам будуть виплачуватися, але через зменшення фінансових надходжень та неповернення позик, наданих під високі відсотки, виплата відсотків по вкладам з часом припиниться.

Можна навести і такий приклад. Кредитна спілка отримувала коши від учасників в якості вступних, пайових і членських внесків. Директор спілки обіцяв видати учасникам кредити без поручителів і документів. Деякі члени спілки захотіли прискорити процес і внесли до 10% від суми майбутньої позики. Однак кредитів ніхто не отримав. Директор організації привласнив собі усі фінансові активи.

Співробітники кредитних спілок нерідко обдурюють своїх роботодавців та привласнюють кошти клієнтів, наприклад, обіцяючи внести їх в касу кооперативів за договорами позики з високою процентною ставкою, натомість виписуючи їм фіктивні квитанції до прибуткових касових ордерів.

Траплялись випадки, коли особи, що працювали на посадах бухгалтерів, навмисно вносили зміни у фінансові документи спілки, аби приховати свої зловживання, наприклад, при оформлені фіктивних договорів передачі особистих заощаджень одна зі співробітниць кредитної спілки заднім числом вносила зміни в касові документи.Пізніше, в ході різних перевірок були виявлені невідповідності в фінансових документах, і аудитори прийшли до висновку, що дані бухгалтерського обліку і звітності не можуть бути використані для оцінки фінансового стану кооперативу.Також в ході перевірки були виявлені великі виплати ряду осіб без договору вкладу та касових документів.

У гонитві за додатковими прибутками, власники та персонал кредитних спілок можуть на власний ризик прийняти рішення про видачу кредиту без ретельної перевірки наявності майна, яке можна було б реалізувати в разі відмови клієнта виплатити позику або відсутності у нього такої можливості.

Якщо перевірка носить формальний характер, то з часом може виявитися, що майна, запропонованого у заставу, насправді немає. Наприклад, клієнт може стверджувати, що у нього є автомобіль, який фактично відсутній (проданий на запчастини або знаходиться на звалищі).

Один із найпоширеніших способів, якими діють зовнішні стосовно кредитної спілки зловмисники, є отримання кредитів у різних організаціях без наміру їх повернути. Інколи оформлення отримання кредитних коштів відбувається на чуже ім'я. Це робиться за допомогою залучення людей, яким обіцяють невелику винагороду за те, щоб взяти кредит на їх ім'я, або оформлення відбувається за допомогою підробленого документа. Страждають від цього самотні, беззахисні люди, ну і звісно, кредитна спілка та її власники.

Ще одним видом фінансових установ, що активно діє на ринку фінансових послуг України, є лізингові компанії. Економічні злочини проти них можуть вчинятись на різних стадіях процесу надання лізингових послуг. На стадії збору документів, шахраї можуть надати неправдиві відомості, що стосуються підприємства-лізингоодержувача. Це можуть бути як підроблені, так і виправлені фінансові звіти (Звіти про фінансовий стан, Звіти про прибутки і збитки) і юридичні документи (Статут, Установчий договір), складені таким чином, щоб задовольняти фінансовим і юридичним вимогамлізингової компанії.Такі документи підвищують ризик прийняття рішення про фінансування компанії, нездатної здійснювати оплату лізингових платежів.

Для попередження шахрайства, керівництву лізингової компанії варто документально упевнитися в наявності предмета лізингу, в законності його існування, а також у відсутності вимог і початку судових дій стосовно предмету лізингу з боку третіх осіб,і перевірити факт того, що предмет лізингу не перебуває в заставі, під слідством, не є об'єктом судового розгляду тощо.

Трапляються випадки, коли лізингоодержувачвказує підставного продавця предмета лізингу. Лізингова компанія переводить гроші на рахунок продавця, який згодом зникає.

Розповсюдженою схемою шахрайства є змова лізингоодержувача з постачальником предмета лізингу з метою завищення вартості майна. Схема досить проста. Здійснюється придбання майна в змові з постачальником за свідомо надвисоку вартість. Лізингоодержувач не сплачує жодного лізингового платежу, повертаючи майно лізингодавцю і при цьому отримуючи різницю, закладену в вартості майна, сплаченого лізинговою компанією.

Відомі також випадки, коли одночасно з завищенням вартості, відбувається уявна крадіжка майна, що приносить шахраям ще більший прибуток (за рахунок різниці реальної ринкової вартості і вартості придбаного майна), а лізингоодержувачу і лізинговій компанії збитки.

Новий вид шахрайства – завоювання ділової репутації лізингової компанії або принцип Троянського Коня.Цей спосіб економічного злочину заснований на придбанні якоїсь «білої» фірми, яка по даним фінансової звітності та іншим параметрам підходить за критеріями і вимогами лізинговій компанії. Цяфірма укладає договір лізингу на майно і виплачує по ньому лізингові платежі в належний термін згідно з графіком, чим заслуговує позитивну кредитну історію. Через 6-9 міс., ґрунтуючись на позитивному співробітництві,лізингоодержувач звертається в лізингову компанію за збільшенням ліміту заборгованості, наприклад, для придбання 5 нових автотранспортних засобів середнього класу.

Лізингова компанія розглядає цю можливість (позитивна кредитна історія, позитивна платіжна дисципліна, позитивна оцінка Служби безпеки), збільшує ліміт і купує для лізингоодержувача нове майно. Лізингоодержувач, в свою чергу, продовжує обслуговувати поточні договори лізингу у визначені терміни і здійснює виплати за новими договорами лізингу 2-3 рази, після чого зникає разом із майном.У таких випадках лізингова компанія несе фінансові та майнові збитки, за рахунок виникнення невідшкодованих інвестиційних витрат і втрати предмета лізингу.

Ще один вид шахрайства проти лізингової компанії – імітація розкрадання – крадіжка, грабіж або розбій.Відбувається імітація крадіжки майна за схемою,

наприклад, помилкового викрадення транспортного засобу. Відомі спроби шахрайства, коли транспортний засіб зникає, нібито, з залишеними в машині документами.

Мають місце випадки викрадення транспорту із крадіжкою документів і ключів у водія транспортного засобу. Трапляються особливі випадки інсценування пограбування (особливо із застосуванням насильства) у формі нападу з викраденням документів і ключів.

За всіма такими схемами відбувається незаконна реалізація майна лізингової компанії, яка згодом зазнає збитків.

Також відомі факти несумлінності контрагента, коли оформлення договору лізингу відбувається на компанію, яка згодом визнаєтьсяфіскальними органами недобросовісною. У такому випадку лізингова компанія не тільки ризикує своїм майном, а й отримує проблеми із зарахуванням ПДВ.

Саме в період економічної кризи, що спостерігається нині в Україні,посилюються ризики здійснення шахрайських дій, оскільки фінансовий тиск з боку банків та інших фінансових інститутів щодо виплат позик посилюється пропорційнодо зростання небезпеки звільнень осіб, що є їх боржниками.

Одним із найпоширеніших та найбільш резонансних видів економічних злочинів, для вчинення якого необхідним є задіяння фінансових установ, є відмивання та легалізація коштів, отриманих злочинним шляхом. У випадку, якщо фінансова установа буде інтегрована у схеми відмивання та легалізації коштів, цей факт не лише матиме катастрофічні наслідки для репутації компаній, але і стане приводом до численних перевірок державних органів нагляду їх діяльності, судових процесів. Таким чином, економічні злочини можуть мати суттєвий негативний вплив на стан економічної безпеки фінансових установ, призводити до втрати ними фінансової стабільності та перспектив подальшого безперебійного функціонування.

На державному рівні завдання протидії економічній злочинності покладено на ряд спеціально створених структур та підрозділів державних органів влади.

Одним із реформаторських кроків було створенняу жовтні 2014 року Національного антикорупційного бюро України — абсолютно нової, незалежної,сучасної правоохоронної структури, покликаної зусією суворістю закону та невідворотністю покарання вести боротьбу з найбільшим внутрішнімворогом — корупцією у владі.Місія Національного антикорупційного бюро: очищення влади від корупції заради побудови та розвитку успішного суспільства та ефективної держави. Корупція є причиною та інструментом для вчинення багатьох видів злочинів у економічній сфері, тому боротьба із нею є важливим завданням національного значення.

Загалом, можна запропонувати такі напрями протидії злочинам у економічній сфері, що становлять загрозу економічній безпеці фінансових установ.

1. Організація сучасних систем економічної безпеки фінансових установ. Важливо, аби така система дозволяла забезпечити захист корпоративних ресурсів установи від економічних злочинів різного характеру – таких, що стосуються привласнення фінансових активів установ чи їх клієнтів, тих, що пов’язані із викраденням, пошкодженням, підміною інформаційних ресурсів, погрозами чи шантажем керівних кадрів компанії з метою отримання певного зиску, тощо.

2. Зважаючи на зростання масштабів кіберзлочинності, фінансовим установам можна рекомендувати перманентно проводити моніторинг соціальних мереж, якими користуються їх співробітники. Соціальні мережі можуть і не становити загрози кіберзлочинності, проте вони можуть бути використані дляпідвищення ефективності засобів соціальної інженерії, якіспрямовані на скоєння злочинів із використанням комп’ютернихтехнологій або сприяють фішингу. Своєчасна перевірка дозволить попередити використаннясоціальних мереж для збору інформації про конкретну особу

(такзвана техніка «цілеспрямованого фішингу») чи длявстановлення шкідливих програм на комп’ютер користувача зметою полегшення подальшого скоєння кіберзлочинів.

3. Одниміз найважливішихінструментів попередженняшахрайства у фінансових установах є підхід «знати зким ви маєте ділові стосунки». Тому важливим елементомпрограм із мінімізації ризиківстає аналіз клієнтів,постачальників та агентів [14, с.12].

4. Новинна і аналітична інформація в засобах масової інформації також може служити одним з найважливіших джерел інформації для цілей виявлення, розкриття і розслідування злочинів у фінансовій сфері. Тому фінансовим установам доцільно запровадити механізми відслідковування відомостей у ЗМІ, які несуть у собі дані щодо шахрайських схем і махінацій з метою попередження подібних випадків у власній діяльності.

5. З метою мінімізації ризику злочинів, що скоюються із застосуванням сили, на кшталт грабунків, збройних нападів тощо, приміщення усіх, навіть найменших фінансових установ (наприклад, ломбардів) належить обладнати охоронною сигналізацією. Для контролю діяльності персоналу, який, як було встановлено, є одним із основних ініціаторів економічних злочинів проти фінансових установ, доцільно встановити камери спостереження, принаймні у тих відділах, працівники яких мають справу із матеріальними, фінансовими цінностями або інформаційними ресурсами.

Існують і специфічні інструменти запобігання та протидії економічним злочинам, що є доцільними для використання конкретними видами фінансових установ.

Так, для банківських установ важливо наполягати на підключенні своїм клієнтам послуги СМС-інформування та рекомендувати їм дотримуватися інших відомих правила при проведенні фінансових трансакцій. Це дозволить своєчасно відстежити несанкціоновані власниками рахунків зняття з них коштів, заблокувати картки і попередити втрати великих грошових сум.

Кредитні спілки з метою протидії економічним злочинам можуть співпрацювати одна з одною, передаючи інформацію про нових учасників, які звернулись за позикою. Дізнавшись, що особавже отримала кредит в іншому місці, кредитна спілка або відмовляє їй у позиці, або приймаються більш суворі законні заходи, якщо у діях особи є ознаки шахрайства. Крім того, кредитним спілкам можна рекомендувати створювати бази даних, в які вносити своїх клієнтів і їх характеристики та кредитні історії. Доцільно підключити до формування такої бази і банківські установи.

Загалом, інформаційна взаємодія між усіма професійними учасниками фінансового ринку є одним із найбільш ефективних інструментів запобігання і протидії економічним злочинам.

Страхові компанії за наявності ефективно організованих процедур прийняття об’єктів на страхування та розслідування страхових подій часто можуть запобігти випадкам шахрайства. Так, факт укладання договору із сумнівною наявністю страхового інтересу у страхувальника повинен привернути увагу андерайтерів у момент оцінки ризиків. Доведення відсутності страхового інтересу в укладанні договору страхування – це не дуже ефективний метод боротьби із шахрайством в особистому страхуванні. Ні укладання договору під час відсутності страхового інтересу, ні подвійне страхування в особистому страхуванні та страхуванні життя не заборонене. Тому для профілактики такого роду випадків представники страховика повинні інформувати клієнтів про те, що неправомірні дії не просто караються, алеі легко розкриваються і у кожному разі супроводжуються відмовою у страховій виплаті.

Також можна запропонувати використовувати обмеження по страховій сумі в договорах особистого страхування. Шахрайство виявляється вигідним для зловмисника тільки тоді, коли страхова сума велика, отже, для профілактики економічних злочинів її розмір потрібно контролювати.

При прийманні на страхування на стадії медичного андерайтингу уважне ставлення до документів, що надаються, дозволяє так само запобігти майбутнім випадкам шахрайства.

При настанні страхового випадку потрібна ретельна перевірка всіх документів, що надаються при зверненні за виплатою. Їхнє уважне вивчення, а також, за необхідності, запити до медичних установ, виїзд на місце страхового випадку тощо дозволять виявити протиріччя в наданих відомостях і викрити обман. Крім того, можна призначити незалежну медичну експертизу[16].

Для протидії економічним злочинам, що вчиняються проти лізингових компаній, можна рекомендувати наступні заходи. Лізингодавець повиненвимагати від лізингоодержувача надання фінансових документів тільки з відмітками фіскальних органів і практикувати обов’язкове вивчення документів за кілька звітних періодів. Аналіз звітності за декілька періодів дозволить відстежити невідповідність фінансових даних (наприклад, різке невиправдане збільшення балансу, фіктивні фінансові вкладення, заборгованість тощо). Для перевірки фінансового стану клієнта фахівцям лізингової компанії доцільно проводити докладний аналіз руху грошових коштів по рахунках і зіставлення його з даними бухгалтерської звітності.

Регулярне проведення тренінгів із менеджерами, які відповідають за ведення проектів, має супроводжуватися обов’язковим повідомленням інформації про можливі санкції, що наступають в разі викриття менеджера в змові з лізингоодержувачем з корисливою метою.

Для запобігання роботі з недобросовісними партнерами, наприклад, постачальниками обладнання, обов’язково повинна ініціюватисьїх перевірка. Для цього повиннівивчатися фінансові та юридичні документи і здійснюватися перевірка керівництва і результатів діяльності потенційного партнера.

У разі відмови продавця майна надати необхідний пакет документів під будь-яким приводом (а їх може бути багато: наприклад, переоформлення документів, перебування документів в сейфі, а керівництва у відрядженні тощо), необхідно негайно повідомити про це лізингоодержувача і припинити

проведення операції з продавцем майна, із занесенням такого постачальника в чорний список.

У випадку будь-яких сумнівів, для мінімізації ризиків необхідно здійснювати остаточну оплату майна тільки після надання оригінальних документів, що підтверджують права на нього. У випадку з лізингом нерухомості, оплату належить здійснювати тільки після переходу та реєстрації права власності на нерухомість на лізингову компанію.

З метою протидії завищенню постачальником вартості майна, перед вступом в угоду, лізинговійкомпанії необхідно проводити моніторинг вартості предмета лізингу як найпростішими способами (інтернет, дзвінки тощо), так і шляхом залучення спеціальної компанії, що спеціалізується на оцінюванні.

У разі, якщо предмет лізингу є специфічним або унікальним, існують такі заходи для захисту інтересів лізинговоїкомпанії, як: договір зворотного викупу з постачальником, де чітко фіксується викупна вартість предмета лізингу на різних часових етапах; збільшення авансу за договором лізингу –це дозволяє зменшити розмір чистих інвестицій лізинговоїкомпанії; коротший (мінімально допустимий) термін лізингу; фінансування майна за схемою, щопередбачає 100% передоплату.

Отже, існування великої кількості видів злочинів у економічній сфері, що можуть мати вплив на інтереси фінансових компаній, призводить до необхідності пошуку ефективного інструментарію протидії їм. Основою для організації належного захисту корпоративних ресурсів фінансових установ від посягань на них зловмисників має бутифункціональна система економічної безпеки. Тому, не зважаючи на наявність державних органів і структур, що намагаються запобігти поширенню економічної злочинності на вітчизняному фінансовому ринку, внутрішні превентивні заходи, направлені на мінімізацію ризику злочинних посягань на активи фінансових установ та їх клієнтів, мають на постійній основі проводитись службами економічної безпеки вітчизняних фінансових посередників, що зайвий раз доводить необхідність їх створення у сучасних умовах господарювання в Україні.

Список використаних джерел:

1. *Осика І.М. Боротьба з фінансовою злочинністю у країнах Європи [Електронний ресурс] / І.М. Осика. – Режим доступу : http://www.univd.edu.ua/_projects/ezloch_kor/docs/stat/osyka.doc.*
2. *Рогозін С. М. Попередження економічної злочинності / С. М. Рогозін // Митна справа. - 2013. - № 4. - С. 17-22.*
3. *Рогозін С. М. Інформаційно-правові засади протидії економічній злочинності / С. М. Рогозін // Боротьба з організованою злочинністю і корупцією (теорія і практика). - 2012. - Вип. 1. - С. 289-294.*
4. *Раєцька Л. В. Попередження злочинності у сфері економіки як засіб забезпечення економічної безпеки держави / Л. В. Раєцька // Боротьба з організованою злочинністю і корупцією (теорія і практика). - 2011. - Вип. 25-26. - С. 274-281.*
5. *Кузьмін Р. Р. Основні напрями загальносоціального запобігання економічній злочинності в Україні / Р. Р. Кузьмін // Науковий вісник Національної академії внутрішніх справ. - 2013. - № 2. - С. 132-136.*
6. *Пчеліна О. В. Щодо використання підприємств у технологіях економічної злочинної діяльності / О. В. Пчеліна // Форум права. - 2011. - № 1. - С. 842-847.*
7. *Ляшенко М. М. Економічні злочини: причини скоєння та їх профілактика / М. М. Ляшенко // Південноукраїнський правничий часопис. - 2012. - № 4. - С. 225-228.*
8. *Медвідь Т. А. Соціально-економічні прояви зростання масштабів злочинності та легалізації коштів, отриманих злочинним шляхом / Т. А. Медвідь // Вісник Університету банківської справи Національного банку України. - 2013. - № 1. - С. 56-60.*
9. *Степанюк Р. Л. Перспективи формування методики розслідування економічних злочинів, що вчиняються в соціально-бюджетній сфері України / Р.Л. Степанюк // Право і Безпека. - 2012. - № 3. - С. 221-224.*
10. *Вівчар О. І. Специфіка особливостей фінансово-економічної безпеки банківського контролю над економічною злочинністю / О. І. Вівчар, В.П. Мартинюк // Вісник Дніпропетровського університету. Сер. : Економіка. - 2013. - Т. 21, вип. 7(1). - С. 53-58.*
11. *Погорелов О. В. Легалізація кримінальних доходів як провідна форма економічної злочинності в умовах глобалізації / О. В. Погорелов // Вісник Дніпропетровського університету. Сер. : Економіка. - 2013. - Т. 21, вип. 7(4). - С. 242-253.*
12. *Гула Л. Ф. Легалізація доходів, одержаних злочинним шляхом, що вчиняються організованими групами, як одна з форм економічної загрози фінансовому ринку / Л. Ф. Гула // Науковий вісник Львівського державного університету внутрішніх справ. серія юридична. - 2014. - Вип. 1. - С. 331-342.*
13. *Економічнізлочини у періодкризи [Електронний ресурс]. – Режим доступу: https://www.pwc.com/ua/en/services/forensic/assets/gecs_2009_report_ukraine_ukr.pdf.*
14. *Всесвітній огляд економічних злочинів : Україна. - 2011.[Електронний ресурс]. – Режим доступу: https://www.pwc.com/ua/uk/press-room/assets/gecs_ukraine_ua.pdf.*
15. *Economic crime: A threat to business globally. – 2014. [Electronicresource]. - Access mode:https://www.pwc.com/gx/en/economic-crime-survey/pdf/pwc-latin-america-economic-crime-survey.pdf.*
16. *Шарвадзе Л. Шахрайство та протидія йому у сфері страхування життя [Електронний ресурс]. – Режим доступу: http://www.ufin.com.ua/analit_mat/strah_rynok/126.htm.*

1.2. РЕЙДЕРСТВО ЯК ОДИН ІЗ ВИДІВ ЕКОНОМІЧНИХ ЗЛОЧИНІВ

МІГУС ІРИНА ПЕТРІВНА, *д.е.н., професор,*
завідувач кафедри менеджменту та економічної безпеки,
МОЛОДЕЦЬКИЙ СЕРГІЙ СЕРГІЙОВИЧ*, здобувач*
кафедри менеджменту та економічної безпеки
Черкаський національний університет імені Богдана Хмельницького

На сьогодні рейдерство визнається однією із найгостріших та найбільш суперечливих проблем вітчизняного бізнесу, що перешкоджає належному функціонуванню не тільки підприємств усіх форм власності, а й органів державної влади України. Широке поширення рейдерства створює суттєву загрозу економічній безпеці України та ставить під сумнів тезу про створення справді високорозвиненої, правової, цивілізованої європейської держави з високим рівнем життя, культури та демократії.

Через відсутність законодавчо закріпленого тлумачення термін «рейдерство» в українській і російській науковій літературі трактується по-різному. І хоча відмінності у тлумаченнях незначні, вони все ж таки мають місце. Більшість авторів до поняття «рейдерство» включають і захоплення підприємств, і дружні та недружні поглинання, навіть деколи й злиття. Це порушення законів логіки. Подібний підхід відбувається через непрофесіоналізм і породжує величезну кількість суперечностей.

В умовах існуючого «теоретичного вакууму» щодо інституту рейдерства український економіст І.М. Макарчук припускає можливість трактувати поняття «рейдерство» «... за аналогією до того, що розуміють під «рейдерством» за кордоном» [2].

Погоджуємося з думкою автора, але за певних умов. У цьому випадку мається на увазі відсутність можливості формування універсального поняття «рейдерство» в контексті існування внутрішньодержавних правових особливостей регулювання системи економічних, у тому числі корпоративних, відносин. Необхідно взяти до уваги й наявність науково-доктринальних

відмінностей у визначенні поняття «рейдерство», зумовлених належністю автора до конкретної наукової школи [2].

Кірєєв А.Ю., визначає рейдерство як систематичну діяльність на ринку корпоративного контролю, спрямовану на несилове правове та не правове отримання контролю над активами інших суб'єктів економічної діяльності із завданням їм економічних та інших збитків.

Представники Національного інституту стратегічних досліджень Варналій З. та Мазур І. визначають рейдерство як недружнє, за межами дії цивільного законодавства, спрямоване проти волі власника захоплення чужого майна [3].

Так, деякі автори звертають увагу не тільки на зовнішні, але й на внутрішньогосподарські передумови поширення рейдерства в Україні. Наприклад, І. Паславський аналізуючи причини виникнення рейдерства звертає увагу на «… велику кількість помилок і порушень в управлінні підприємствами, тобто наявність значного резерву формальних приводів для рейдерських атак» [4].

Проблемі визначення причин поширення рейдерства присвячені роботи представників економічної науки близького зарубіжжя. Наприклад, Тарханова З.Є. виокремлює такі передумови розвитку рейдерства: нечітка, непрозора система реєстрації прав власності; високий рівень чиновницької корумпованості; високий ступінь недосконалості ринку корпоративного контролю на фоні зростання його сумарних значень у валового внутрішнього продукту; недооцінка активів середніх і малих публічних акціонерних товариств, чиї акції не є інструментом ринку корпоративного контролю, що призводить до зростання конкуренції при оцінці альтернатив та рівня витрат угод активів в секторі середніх і малих публічних акціонерних товариств [5].

Подібного погляду дотримуються й інші українські дослідники. Так, на думку Б.М. Грека, рейдерство в сучасному розумінні – це недружнє поглинання підприємств і компаній, перерозподіл власності й корпоративних прав.

Іншими словами, рейдерство – це недружнє, поза межами дії цивільного законодавства, спрямоване проти волі власника захоплення чужого майна на

користь іншої особи, установлення над майном повного контролю нового власника в юридичному і фізичному розумінні з використанням корумпованості чиновників та (або) із застосуванням сили» [6].

Розміщення інституту рейдерства виключно за межами правового поля конструктивно критикується з боку деяких авторів. Так, український дослідник М.А. Колесник акцентує увагу на можливості здійснення недружнього захоплення чужого майна, а також установлення над ним повного контролю в межах чинного законодавства [7]. Вважаємо таку критику цілком обґрунтованою.

Інші автори, досліджуючи інститут рейдерства, доходять висновку про можливість його розміщення в незаконній, законній, або так званій «напівзаконній» сферах.

До речі, прибічником такого підходу є російський дослідник Н. Лопашенко, який стверджує, що рейдерство – це методика заволодіння чужою власністю, що ґрунтується на мистецтві менеджменту та корпоративних юристів і становить ретельно сплановану систему діяльності, спрямовану на отримання чужої компанії, що здійснює підприємницьку та (або) інші види економічної діяльності. На думку автора, рейдерство, містить поєднання незаконних, напівзаконних (протиправних, але таких, що не знайшли законодавчої заборони і не прописаних у законі) і законних способів придбання привабливої, але чужої власності [8].

На окрему увагу заслуговує існуюча в економічній науці думка про подвійну природу рейдерства, згідно з якою рейдерство – це спосіб перерозподілу власності, що, в принципі, є кримінальним, а за формою набуває деяких форм юридичних процедур [9].

Ще більш категоричного погляду про можливість легальних форм рейдерської діяльності дотримуються інші вітчизняні дослідники. Вони зазначають, що «рейдерство» в класичному розумінні становить реалізацію заходів із придбання чужого підприємства, переважно в межах чинного законодавства.

Незважаючи на цю обставину, рейдер утім діє всупереч волі керівництва й акціонерів підприємства – об’єкта рейдерського захоплення.

Така специфіка рейдерської активності зумовлює її віднесення до об’єктивних процесів, що сприяють динаміці економічного росту і побудові конкурентоспроможної економіки [10].

На окрему увагу заслуговує позиція деяких авторів, зокрема С. Симакова, про безпідставність самого віднесення поняття «рейдерство» до наукових, у тому числі економічних та юридичних категорій [11].

Підтримуючи вищезазначену точку зору, І. Головань лише обмежується асоціацією поняття «рейдерство» з «модним» терміном [12]. Такий авторський підхід аргументований відсутністю відповідальності, що передбачена чинним законодавством за здійснення рейдерських дій, а отже, й неприпустимістю нормативно-правової можливості боротьби із зазначеним негативним феноменом дійсності.

Аналіз існуючих поглядів на економіко-правову природу «рейдерства» підтверджує факт переважного застосування широкого підходу до визначення цього поняття.

Так, український правознавець О. Бєліков, використовуючи цей підхід, характеризує рейдерство як послідовний алгоритм операцій, що дозволяє за допомогою прогалин у законодавстві отримати у володіння певний капітал (у більшості випадків – підприємство). Зауважимо, що реалізація подібної моделі часто супроводжується виведенням активів з володіння законних власників. Такий факт не виключає факт виведення рейдерських атак за межі легітимних суспільних відносин [13].

Використання широкого підходу до визначення рейдерства часто призводить до ототожнення рейдерства з такими поняттями, як «недружнє поглинання», «корпоративний шантаж» і «незаконне встановлення контролю над підприємством».

Зауважимо, що в економічній науці близького зарубіжжя також мають місце прецеденти повного ототожнення понять (термінів) «недружнє

поглинання», «корпоративний конфлікт», «захват підприємства» та «рейдерство». Непоодинокі й випадки віднесення в пострадянській економічній науці до рейдерства процесів «грінмейлу».

Так, Полушкін О.А. вважає вищезазначені поняття синонімами [14]. Разом з тим, автор безпосередньо відносить до рейдерства шахрайство, підробку документів, реприватизацію та ініціювання банкротства. Проаналізуємо економіко-правову сутність зазначених понять і визначимо доцільність їх ототожнення.

В основу визначення економіко-правової природи поняття «недружнє поглинання» покладена британська й американська модель організації ринку корпоративного контролю.

Обидві моделі ґрунтуються на визнанні поглинання – дружнього і недружнього – позитивним явищем, що за належного регулювання сприяє швидкому й ефективному перерозподілу виробничих і фінансових ресурсів з мінімальними втратами на користь більш ефективних менеджерів. Механізм поглинання розглядається як один з найпотужніших «двигунів» американської та британської економіки.

Загроза втратити роботу внаслідок недружнього поглинання забезпечує істотну мотивацію для менеджерів підприємства, зумовлює їх працювати чесно та ефективно на користь акціонерів.

Незадовільні результати діяльності підприємства, відсутність дивідендів, нехтування інтересами акціонерів веде до того, що таке підприємство стане легкою здобиччю для загарбника, а його акціонери з готовністю продадуть свої акції, натомість менеджерам і директорам доведеться шукати нову роботу [15].

Дружнє поглинання (friendly take-over) є операцією двох юридичних осіб щодо приєднання однієї юридичної особи до іншої. Аналогією дружнього поглинання можна вважати приєднання.

Майже 95 % усіх злиттів і поглинань відбуваються за взаємною згодою сторін. У цьому випадку керівництво підприємства, що поглинається, позитивно ставиться до перспективи поглинання, погоджується не чинити опір

поглинанню та рекомендує своїм акціонерам прийняти пропозицію підприємства-агресора, яке поглинає, про продаж йому своїх акцій [15].

Оскільки поглинання, в тому числі і дружнє, неминуче призводить до змін у менеджменті підприємства, то позитивне ставлення керівництва підприємства-мети до перспективи втрати ним своїх повноважень, прав і компетенцій є, радше винятком, ніж правилом.

Процедура поглинання відбувається не лише за взаємною згодою, але й з виникненням конфлікту, наприклад, усупереч бажанню менеджменту, але з відома акціонерів підприємства. Останній випадок отримав назву недружніх (або ворожих) поглинань (hostile take-over).

Недружнє поглинання – це встановлення над підприємством або активом повного контролю як в юридичному, так і у фізичному сенсі всупереч волі менеджменту або власника цього підприємства, або активу [15].

Як зазначає автор, недружнє поглинання відбувається проти волі власників або керівництва підприємства, але це не означає, що поглинання відбувається у незаконний спосіб. Тобто недружнє поглинання відрізняється загалом від дружнього опором менеджменту або власників підприємства-мети. Відповідно, у цьому випадку керівництво підприємства-мети налаштовано проти поглинання, намагається зірвати поглинання, зробити його невигідним для поглинача та закликає акціонерів не продавати свої акції підприємству-агресору.

В основі недружніх поглинань завжди лежить конфлікт зацікавлених осіб, який, наприклад, може виникати через порушення прав міноритарних акціонерів або, навпаки, через їхній шантаж з метою дорожчого продажу своїх акцій (в зарубіжній практиці називається грінмейлом) [15].

Майнові суперечки, фактичним предметом яких є встановлення контролю над підприємствами шляхом недружнього поглинання, стали звичайною практикою підприємницького життя.

У деяких випадках мета недружніх (або ворожих) поглинань – продаж активів підприємства та його ліквідація. Здебільшого на захоплених

підприємствах проводиться рестрктуризація, що спричиняє зміну менеджменту, продаж непрофільних активів підприємства, реструктуризацію боргів, скорочення витрат та оновлення основних виробничих фондів. Таким чином, контроль над підприємством переходить до ефективного власника.

Класичні рейдери сприяють економічному розвитку, відсторонюючи від управління бізнесом неефективний менеджмент, перешкоджаючи зловживанням великих акціонерів і реструктуруючи неефективно працюючі підприємства. До того ж, сьогодні немає чітких критеріїв, за якими те чи інше поглинання підприємства можна вважати протиправним, у тому числі й злочинним.

Способи недружнього поглинання ґрунтуються на використанні чинного законодавства і їхнє використання не передбачає його порушень або квазізаконного удавання до чинних законів (рис. 1.1).

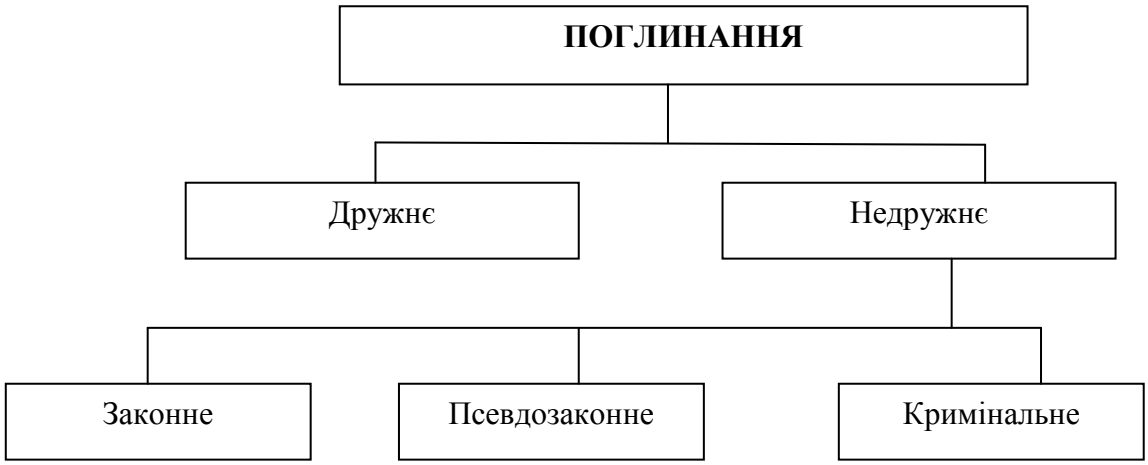


Рис. 1.1. Види поглинання підприємства

Джерело: систематизовано автором [16]

Факт поширення під час недружнього захоплення технологій шантажу міноритарних акціонерів задля дорожчого продажу акцій зумовлює виникнення різноманітних алгоритмів корпоративного шантажу.

В економічній літературі під корпоративним шантажем розуміють дії, спрямовані на порушення нормального функціонування акціонерного товариства, що звичайно здійснюються дрібним акціонером з метою

досягнення викупу належного йому пакету акцій за ціною, яка значно перевищує ринкову [17].

Деякі автори, зокрема М.Г. Іонцев, безпосередньо відносять корпоративний шантаж до грінмейлу [18]. На думку представників такого теоретичного підходу, сутність будь-якого корпоративного шантажу полягає в тому, щоб шляхом різних формально законних способів змусити придбати пакет акцій, що належить грінмейлеру, за завищеною ціною.

Під незаконним встановленням контролю над підприємством, як правило, розуміють суспільно небезпечне, протиправне діяння, пов'язане з незаконним придбанням права володіння, та (або) використання, та (або) розпорядження активами (часткою активів) юридичної особи, або пов'язане з установленням контролю над юридичною особою шляхом незаконного придбання права володіння, та (або) використання, та (або) розпорядження частками учасників юридичної особи в уставному капіталі [19].

У будь-якому випадку незаконне встановлення контролю над підприємством асоціюється з активною діяльністю заподіяння шкоди правам або законним інтересам власників акціонерного товариства, що суперечить їх волевиявленню та загрожує безпеці особистості, суспільства та держави.

Слід вважати, що повне ототожнення рейдерства з різними варіаціями недружнього поглинання досить сумнівне. Контраргументом подібного підходу є англосаксонський підхід до визначення недружнього поглинання. Згідно з останнім, недружнє поглинання – це легітимне встановлення контролю (придбання) над контрольним пакетом акцій підприємства на ринку цінних паперів, його реорганізація або ж продаж. При цьому, зарубіжною теорією зовсім не виключаються активні дії, спрямовані на протидію встановленню зазначеного контролю (проведення реорганізації) з боку топ-менеджменту або акціонерів компанії.

Звертаючи увагу на цю обставину, О.А. Полушкін справедливо зауважує, що загалом, поглинання – це процес, у результаті якого активи компанії переходять у власність покупця, а зовсім не «загарбника» [20].

На феномен ототожнення понять «недружнє поглинання», «корпоративний конфлікт», «захват підприємства», «рейдерство» та «грінмейл» звертають увагу і деякі зарубіжні автори.

Так, К.О. Гуман пояснює факт ототожнення зазначених термінів тим, що в державах з розвиненою ринковою економікою не існує такого поняття, як рейдерство, а недружні захвати виявляються в зовсім інших формах, з абсолютно іншою специфікою, але російські автори переважно користуються зарубіжною термінологією, визначають за її допомогою процеси російського рейдерства [21].

У свою чергу, деякі автори виводять інститут недружнього поглинання з площини легітимних дій суб’єктів корпоративних відносин.

Так, С.Г. Мартинов у своїй дисертації асоціює недружнє поглинання з установленням контролю над господарським товариством через нелегітимну зміну органів його управління та / або використання боргових зобов'язань та / або за допомогою придбання прямо або опосередковано активів і цінних паперів товариства всупереч волі інших акціонерів [22].

Слід вважати, що незаконний характер установлення корпоративного контролю в деяких випадках характерний саме для рейдерства, а не для інституту недружнього поглинання.

Зауважимо, що ряд авторів відносить рейдерство до незаконних дій, які здійснюються з метою заволодіння майном іншого суб’єкта. Такий погляд пропагують українські дослідники П.В. Берназ та О.О. Середа [23].

Визначаючи економіко-правову суть рейдерства, деякі російські економісти (у тому числі на дисертаційному рівні) відзначають його не правовий характер [24].

Погоджуємось з Бурбело О.А. та іншими, які вважають, що попри певну схожість економіко-правової природи, «рейдерство» та «недружнє поглинання» - різні поняття. Зважаючи на це, слід погодитися з фахівцями в галузі безпеки, що рейдинг (рейдерство) – це процес, а поглинання – це результат [25].

Вивчення процесу здійснення рейдерського захоплення дозволило виділити такі *види рейдерства* залежно від сегмента ринку, де діє підприємство-мета та підприємство-агресор, що зумовлюють його вітчизняну специфіку (рис. 1.2).

Горизонтальне рейдерство має на меті створення інтегрованої структури підприємств зі схожими видами діяльності, що забезпечує економію за рахунок ефекту масштабу та синергії. Зазвичай такі захоплення відбуваються на підприємствах, що працюють в одному сегменті ринку (в одній галузі) та спеціалізуються на виробництві подібної продукції або наданні подібних послуг.

Рис. 1.2 Види рейдерства залежно від сегмента ринку, де діє підприємство-мета та підприємство-агресор, що зумовлюють його вітчизняну специфіку

Джерело: Складено автором на основі [16]

Метою горизонтального рейдерства є – збільшення сегменту ринку, а отже, ступеня концентрації в галузі і, як наслідок, витіснення з ринку конкурентів [26].

Горизонтальні рейдерство за своєю метою поділяється на два види:

а) що розширює географію ринку збуту підприємства-агресора, проводиться за допомогою заволодіння активами підприємства-мети, яке виробляє ідентичну з підприємством-метою продукцію, але працює на інших географічних сегментах ринку;

б) що розширює асортимент підприємства-агресора, проводяться за допомогою заволодіння активами підприємства-мети, яке виробляє подібну, але не абсолютно ідентичну продукцію.

Вертикальне рейдерство, мета якого - створення багаторівневої інтегрованої структури підприємства, з метою мінімізації фінансових витрат [27]. Обмежує цей вид рейдерства вимога стійкості технологічних зв'язків і ймовірність економічної невигідності інтегрування. Також технологічні зміни можуть зробити якусь ланку інтегрованої структури непотрібною або менш ефективною, ніж передбачалося.

Прикладом вертикального рейдерства є захоплення сталеливарною компанією підприємства з видобутку залізної руди, вугілля, або нафтовидобувною компанією нафтопереробного підприємства.

Споріднене (або концентричне) рейдерство, що зазвичай визначають як захоплення підприємств «подібних за природою та діями». Під час цих захоплень підприємство-агресор і підприємство-мета пов'язані між собою базовою технологією, виробничим процесом або через ринкову нішу [28].

Споріднене (або концентричне) рейдерство значно підвищує рівень монополізації відповідного сектору ринку та стримує його розвиток.

Конгломеративне рейдерство, за якого захоплюється підприємство, що ніяк не стикається з діяльністю підприємства-агресора як на сегменті ринку, так і у виробничо-постачальницьких зв’язках. Конгломерат є об’єднанням технологічно непов’язаних виробництв, для якого характерні частий продаж і купівля активів різного виду. Зазвичай підприємство-агресор переслідує мету диверсифікації своєї діяльності [28].

Вважаємо, що рейдерство передусім доцільно розглядати з точки зору правових наслідків його здійснення, розрізняючи законне та незаконне.

Законне рейдерство або рейдерство у класичному його тлумаченні – це заволодіння майном, бізнесом, що здійснюється цілком законними методами, зокрема, за допомогою скупки (міни, дарування) акцій або часток у статутному фонді підприємства, проведення додаткової емісії акцій, скупки боргів підприємства, що поглинається, для формування конкурсної маси з метою ініціації справи про банкрутство підприємства-мети, реприватизації, сутність якої полягає в судовій відміні приватизації та подальшому перерозподілі власності.

Незаконне рейдерство або рейдерство, що сформувалося на пострадянському просторі, – це заволодіння майном і бізнесом за допомогою методів, які суперечать чинному законодавству.

У свою чергу, незаконне рейдерство поділяється на кримінальне й некримінальне, залежно від наявності передбаченого кримінальним законодавством країни складу злочину в діях загарбника [29].

У контексті вищезазначеного досить обґрунтованою є думка Н. Гуторової, яка виділяє два види рейдерства – «біле» і «чорне» – і акцентує увагу на доцільності використання терміна «рейдерство» лише для позначення фактів протиправного захоплення підприємств [30].

Мігус І.П. зазначає, що, рейдерство – це незаконне захоплення підприємства з метою заволодіння його активами та з використанням незаконних методів і засобів (кримінальне рейдерство) або недружнє чи вороже поглинання підприємства з використанням законних (правових) засобів з тією самою метою. Це визначення охоплює всі форми та види рейдерства, так зване «біле», «сіре» та «чорне» рейдерство [31]:

- «чорне» рейдерство – припускає використання незаконних схем присвоєння власності із застосуванням силових методів, таких як шантаж, захоплення співробітників підприємства в заручники, підкуп представників відповідальних відомств, силове захоплення території підприємства,

фальсифікація рішень суду, статутних документів, протоколів зборів акціонерів тощо;

- «сіре» рейдерство – припускає поєднання формально законних і незаконних дій, таких як форсування прийняття рішень представниками судової влади, створення атмосфери, при якій нормальне функціонування робочого процесу стає неможливим, розміщення компрометуючих матеріалів у ЗМІ, неформальний тиск на відповідальні за ситуацію осіб, адміністративний ресурс, "сарафанне радіо", затягування строків через надумані причини, різні відволікаючі маневри тощо;

- «біле» рейдерство – припускає дії, що формально залишаються в рамках закону, наприклад, використання у своїх цілях законодавчих норм, маніпуляції суспільною думкою, схиляння на свою сторону представників органів влади шляхом неформальної комунікації, заохочення страйків серед співробітників підприємства, "злив" компрометуючої керівництво підприємства звітності у відповідні податкові органи й контролюючі інстанції тощо.

З іншого боку, в сучасному цивілізованому світі розповсюджений тільки легальний тип рейдерства, який дозволений, контрольований і врегульований законом. Таким чином, поняття «рейдерство» в західноєвропейському розумінні, як правило, немає негативного значення.

Враховуючи вищезазначене, вважаємо за доцільне систематизувати види та форми рейдерства, ґрунтуючись саме на правовому підході до його ідентифікації та представити на рис. 1.3.

Найбільш розповсюдженими методи здійснення рейдерських захоплень в Україні є:

1) скупка акцій;

2) зміна керівництва;

3) помилки при приватизації.

Рис. 1.3. Види рейдерства в Україні

Джерело: систематизовано автором [28-31].

При реалізації першого методу рейдери скуповують 10-15% акцій, а цього зазвичай достатньо, аби ініціювати збори власників і ухвалити потрібне рішення, наприклад щодо зміни керівництва. Типовим є приклад корпоративного конфлікту, що виник навколо публічного акціонерного товариства «Універмаг «Україна». Він був пов’язаний з низкою неправомірних дій представників колишнього менеджменту універмагу та інших осіб і мав на меті відсторонення від контролю за ситуацією на підприємстві міжнародного акціонера, якому належить 92,7% статутного капіталу товариства. Відбувалися маніпуляції з організацією засідань наглядової ради та загальних зборів акціонерів, що давало можливість особам, які мали значно меншу частку в статутному капіталі, вчиняти дії, що суперечили інтересам інших акціонерів [32].

При використанні другого методу, змінюється через наймане керівництво, яке може просто «виводити» активи на підконтрольні рейдеру структури або

бере кредити під заставу власності під завищені відсотки. Ситуація, що склалася навколо ПАТ «Готельно-туристичний комплекс «Інтурист-Закарпаття» є яскравим прикладом такого способу захоплення. Прокуратурою Закарпатської області порушено і розслідуються кримінальні провадження за ознаками вчинення кримінальних правопорушень у сфері службової діяльності при переоформленні складу органів управління комплексу. Правопорушення полягає в тому, що голові правління було пред'явлено сфальсифікований протокол загальних зборів акціонерів, згідно з яким призначено новий склад правління, а також протокол наглядової ради у складі, суттєво відмінному від обраного на загальних зборах. Крім того, було змінено охорону готельного комплексу та встановлено контроль за установчими документами і печаткою підприємства [33].

Використання третього методу можливе тоді, коли підприємство приватизується незаконним шляхом. Прикладом є ситуація, що склалася навколо сільськогосподарського ТОВ «Бучанський». Під час оформлення землевпорядної документації ТОВ «ВВ-Брік Траст» на земельні ділянки розміром 18,4370 га було порушено вимоги Земельного кодексу України та Постанови КМУ від 26 травня 2004 р. № 677, якою затверджено Порядок розробки проектів землеустрою щодо відведення земельних ділянок. Зокрема, проекти землеустрою з органами містобудування та архітектури не погоджувались та головою сільської ради не підписувались. Крім цього, на більшості земельних ділянок, переоформлених та переданих до ТОВ «ВВ-Брік Траст», розташовано нерухоме майно колишнього КСП, право власності на яке зареєстроване в Києво-Святошинському БТІ за рядом фізичних та юридичних осіб. При цьому більшість власників об'єктів нерухомості мають чинні рішення сесій сільської ради про надання дозволів на розробку проектів землеустрою щодо відведення їм в оренду ділянок. Більше всього рейдерських атак було здійснено у передкризові 2007 – 2008 роки. У цей період зареєстровано сотні протиправних захоплень підприємств, підставою для яких стали ухвали і рішення судових інстанцій. З цієї кількості 11 підприємств мали стратегічне

значення для економіки та безпеки держави. Зокрема, йдеться про ВАТ «Турбоатом» (м. Харків), ВАТ «Запоріжжяобленерго», Державну акціонерну холдингову компанію «Чорноморський суднобудівний завод» [34].

Зазначені вище методи є так званими «класичними», проте останнім часом в умовах фінансово-економічної кризи традиційне рейдерство, засноване на юридичних маніпуляціях, пішло на спад, а натомість використовуються захоплення, що ґрунтуються на економічних моделях та використанні різноманітних інформаційних ресурсів.

Вважаємо, що новітні форми рейдерства доцільно об'єднати у дві основні групи:

1) боргові (з використанням кредиторської заборгованості, бюджетної заборгованості та з використанням застави);

2) корупційні [35].

Окремо вони застосовуються досить рідко, найчастіше можна зустріти їх комбінації між собою.

У схемах з використанням *кредиторської заборгованості* найважливіше – це отримання інформації про фінансовий стан підприємства, а точніше - про фінансову стійкість та її межі. Після отримання якої, рейдер приступає до скуповування кредиторської заборгованості підприємства, і чим більший її обсяг він консолідує, тим більше у нього шансів поглинути бізнес без особливого ризику (рис. 1.4).

Так, якщо у підприємства є кілька дрібних заборгованостей, рейдер скуповує їх і пред'являє до одноразової оплати. Тут є показовою ситуація, що склалася навколо ДП НАЕК «Енергоатом». У період з 2002 року і дотепер на території України, Республіки Молдова та деяких країн Європейського Союзу компанією «Remington Worldwide Limited» (Гібралтар) і компаніями, яким вона передала право на здійснення вимог проти України та ДП «НАЕК «Енергоатом», були ініційовані численні судові процеси.

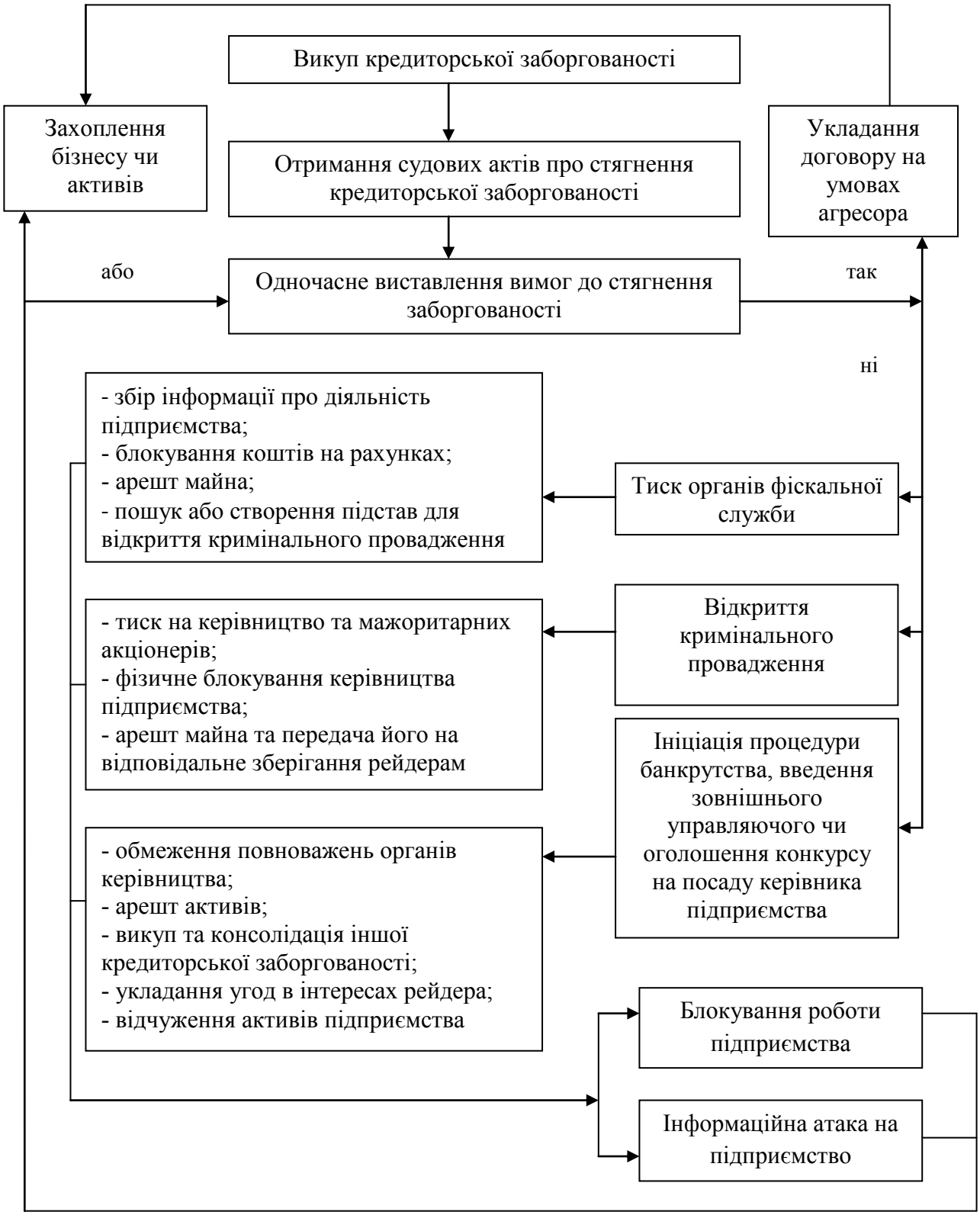


Рис. 1.4. Схема здійснення рейдерського захоплення з використанням кредиторської заборгованості

Джерело: складено автором на основі [36-37]

Головна мета полягала в заволодінні активами ДП «НАЕК «Енергоатом» та інших енергетичних компаній і банків України. Прикрим є те, що зазначені незаконні схеми заволодіння коштами та майном були «узаконені» рішеннями судів Республіки Молдова, відповідно до яких визнано борг ДП «НАЕК «Енергоатом», ПАТ «Дніпрообленерго», ПАТ «Одесаобленерго», ТОВ «Луганське енергетичне об'єднання», «Миколаївобленерго» на суму понад 350 млн. грн. [38].

Схема використання *застави* з метою поглинання бізнесу або активів - це по суті додатковий метод, який використовується при рейдерському захопленні підприємства, в тому числі і через права на кредиторську заборгованість. Учасниками реалізації цієї схеми зазвичай виступають банки-кредитори, з якими компанія уклала договір про кредитування під заставу майна. Вони можуть діяти від свого імені або залучити групу професійних рейдерів (рис. 1.5).

За наведеною вище схемою було здійснено рейдерське захоплення ТОВ «Черкаська продовольча компанія» (ТОВ «ЧПК»). Так, Господарським судом Черкаської області було ухвалено рішення про визнання ТОВ «ЧПК» банкрутом і відкриття ліквідаційної процедури за поданням АТ «Укрексімбанк», який виступав в ролі кредитора підприємства, яке отримало мільйонний кредит під заставу своїх майнових комплексів. Також було судом скасовано заборони на майно боржника, накладені ухвалою суду від 1 червня 2011 року та будь-які інші обмеження щодо розпорядження майном цього боржника.

А 17 червня 2015 року близько 20 години визначений у постанові суду арбітражний керуючий здійснила дії щодо виконання вищевказаного рішення господарського суду та разом зі своїм помічником за підтримки невідомих 70 осіб, грубо порушуючи громадський порядок, із застосуванням фізичної сили, потрапили до приміщення ТОВ «ЧПК».

Рис. 1.5. Схема здійснення рейдерського захоплення з використанням заставного майна підприємства

Джерело: складено автором на основі [36-37]

Соснівський РВ в м. Черкаси за цим фактом вніс відомості до Єдиного реєстру досудових розслідувань за ознаками кримінального правопорушення, передбаченого ч. 2 ст. 296 КК України (хуліганство, тобто грубе порушення громадського порядку з мотивів явної неповаги до суспільства, що супроводжується особливою зухвалістю та винятковим цинізмом, вчинене групою осіб) [34].

Схема з *бюджетною заборгованістю* являє собою яскравий приклад використання механізмів примусу держави в приватних інтересах. Для її реалізації агресор вступає в змову з співробітниками того відомства, у повноваженнях якого виявилися борги підприємства, що впливають на його фінансовий стан. Ними можуть виявитися будь-які державні організації, куди підприємство повинно здійснювати відрахування. Наприклад, Державна фіскальна служба, Пенсійний фонд тощо. Однак найчастіше відомством тиску обирається Державна фіскальна служба, права якої чітко прописані в Податковому кодексі України, та є досить широкими щодо економічної діяльності підприємства. При цьому видима частина активної діяльності може представлятися як самостійна робота державного органу з примусового погашення кредиторської заборгованості перед бюджетом (рис. 1.6).

Що стосується *корупційних методів* протиправного захоплення підприємств і бізнесу, то вони є досить актуальними для України, привабливими для рейдерів та відносно прості у виконанні. Ця схема являє собою одну з найбільш примітивних, втім, її примітивність не знижує її ефективність, оскільки основний її важіль досить жорсткий – це позбавлення керівників і власників об'єкта волі до опору і добровільний вибір продажу бізнесу замість притягнення до кримінальної відповідальності.

Поглинання бізнесу за цією схемою може бути організовано як традиційним замовником поглинання, із залученням спеціалізованих рейдерських компаній, так і самостійно професійним агресивним учасником ринку злиттів і поглинань, якому необхідно вигідно реалізувати накопичений корупційний силовий адміністративний ресурс [39].

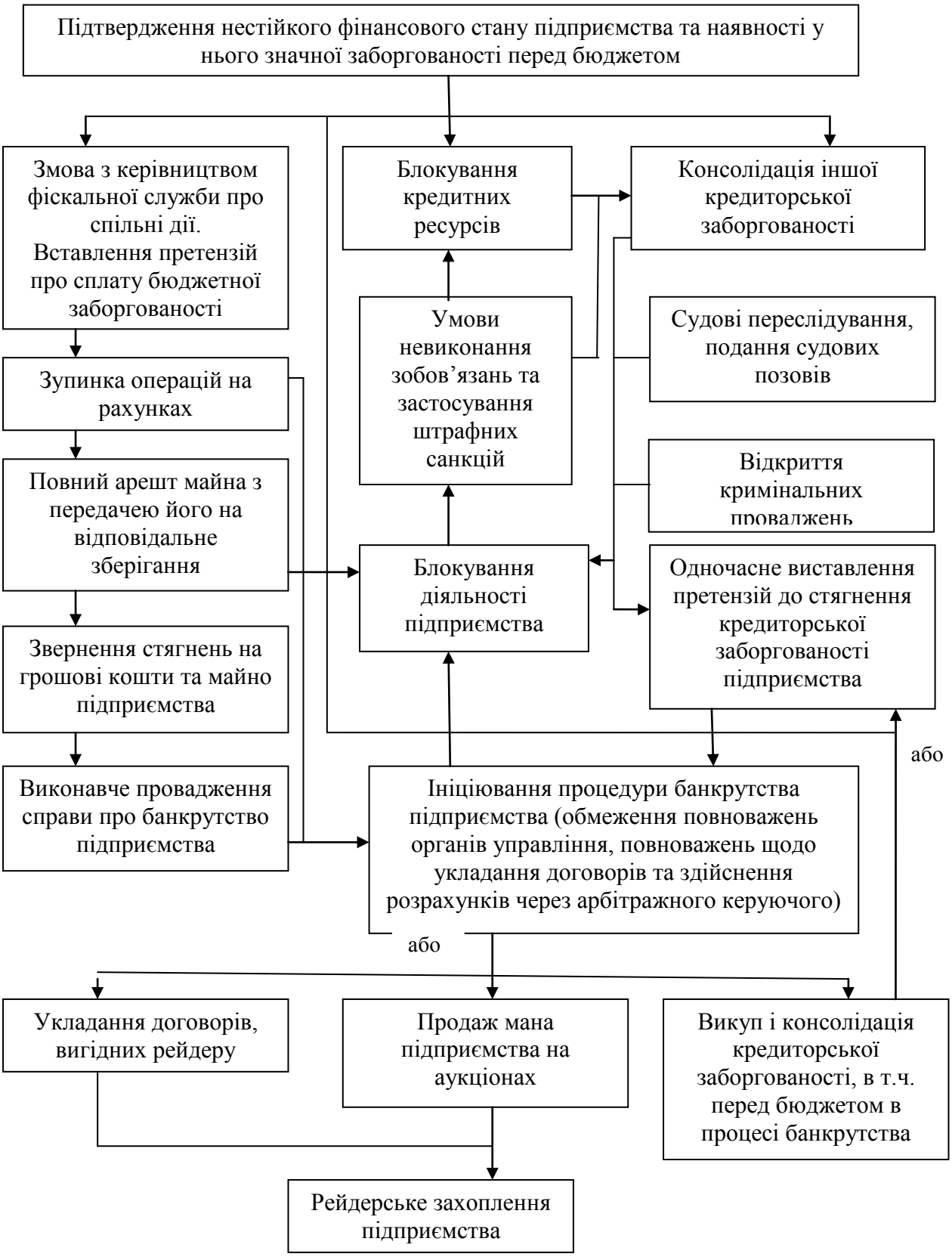


Рис. 1.6. Схема здійснення рейдерського захоплення з використанням бюджетної заборгованості

Джерело: складено автором на основі [36-37]

Корумповані співробітники правоохоронних органів, а це, як правило, співробітники слідчих підрозділів і прокуратури, виступають в реалізації такої схеми як активні співучасники. Однак їх співучасть важко довести, оскільки їх дії виглядають як самостійні.

Отже, аналіз особливостей здійснення рейдерських захоплень в Україні показав, що в більшості з них суттєву роль відіграє корупційна складова із залученням органів державної влади різних рівнів.

Аналізуючи динамку рейдерських захоплень, які відбулись в Україні в період з 2011 по 2015 рр., та кількості рейдерських фірм, слід зазначити, що не дивлячись на невелику кількість останніх, їх діяльність на початок 2011 р. була досить значною. Але завдяки зростанню публічності, інформаційної прозорості та результатів діяльності керівництва акціонерних товариств, їх кількість зменшилась (рис. 1.7).

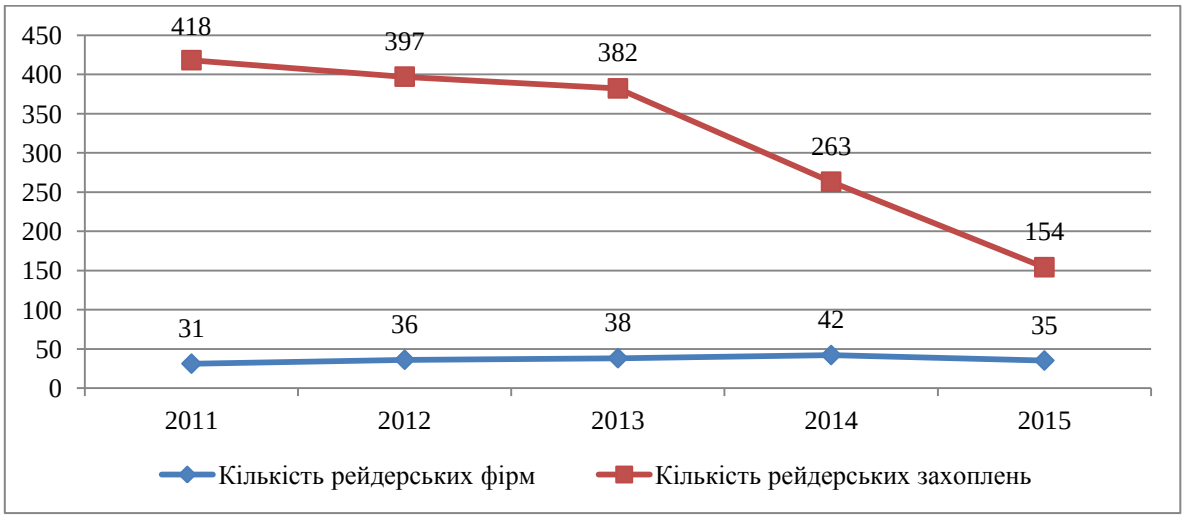


Рис. 1.7. Динамка рейдерських захоплень, які відбулись в Україні в період з 2011 по 2015 рр., та кількості рейдерських фірм

Джерело: складено автором за даними Державної служби статистики та інтернет-сайту Антирейдерського союзу підприємців України [40-41]

Аналіз проблеми виникнення та розвитку рейдерства дозволив дійти висновку, що рейдерство не є виключно українським феноменом в сучасних умовах. Однак інституалізація рейдерської активності в Україні має свої

специфічні відмінності, пов’язані з передумовами виникнення й особливостями подальшого розвитку цього негативного феномену сучасного господарювання.

Вважаємо, що до основних передумов розвитку рейдерства в Україні слід віднести наступні:

- низький рівень правової культури та правовий нігілізм на всіх рівнях (серед суб’єктів господарювання, представників органів влади та в суспільстві загалом; низький рівень ступеня відкритості суспільства і економіки);
- високий рівень корумпованості правоохоронних, судових і дозвільних структур;
- недосконалість ринкових інструментів перерозподілу власності та велика кількість управлінських внутрішньогосподарських помилок («резерв формальних приводів рейдерства»);
- відсутність регулярної ринкової оцінки ліквідних активів підприємств;
- ефемерність української моделі фондового ринку та відсутність чіткої реалізації вільного обігу акцій;
- нечітка і непрозора система реєстрації прав власності;
- низька інформаційна транспарентність підприємств;
- зростання корпоративних конфліктів, пов’язаних з недосконалістю законодавства у сфері корпоративних відносин;
- недосконалість правової системи й відсутність державних інституцій ефективного захисту прав власності в Україні.

Отже, вивчення передумов, особливостей, видів та форм рейдерства дозволило з'ясувати щільний зв'язок між рейдерство та економічною безпекою підприємства та запропонувати авторське трактування даного поняття.

Вважаємо, що рейдерство – процес спрямований на заволодіння активами підприємства шляхом використання законних та/або незаконних заходів, що негативно впливає на його фінансовий стан та економічну безпеку, вчинений відповідними суб’єктами.

На наш погляд, саме таке визначення розкриває поняття рейдерство з позицій економічної безпеки та вказує на способи (законні чи незаконні),

об'єкту захоплення (саме підприємство чи його окремі активи) та результат (втрата економічної безпеки), що дозволить більш чітко ідентифікувати відповідні загрози та знайти шляхи їх нейтралізації.

Список використаних джерел:

1. *Макарчук І. М. Рейдерство, як одна з форм тіньової економіки держави та його наслідки [Електронний рисурс] // Економічний вісник університету. Збірник наукових праць. – 2010. – № 1. – Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/evu/2010_15_1/Makarch.pdf*
2. *Киреев А. Ю. Рейдерство в Российской экономике: сущность, тенденции и возможности противодействия. Автореф. дис. … канд. экон. наук: 08.00.05 / А. Ю. Киреев. – М., 2008. – 21 с.*
3. *Варналій З., Мазур І. Основні передумови та шляхи подолання рейдерства в Україні. Аналітична записка Національного інституту стратегічних досліджень / З. Варналій, І. Мазур [Електронний ресурс]. – Офіційний сайт Національного інституту стратегічних досліджень. – Режим доступу: http://old.niss.gov.ua/Monitor/juli/1.htm*
4. *Паславський І. Основні етапи протидії українському бізнесу. Роль і позиції ЗМІ / І. Паславський // Вісник Львівського університету. – 2011. – Вип. 34. – С. 159-162*
5. *Тарханова З. З. Функционирование института рейдерства в РФ: автореф. дис. на соискание уч. степени канд. экон. наук: спец. 09.00.01 / З. З. Тарханова. – Владикавказ, 2008. – 21 с.*
6. *Грек Б. М., Грек Т. Б. Поняття та історичні передумови розвитку рейдерства в Україні / Б. М. Грек, Т. Б. Грек // Адвокат. – 2010. – № 9. – С. 29-34*
7. *Колєсник М. А. Рейдерство в Україні: Загальна характеристика та основні тенде- нції розвитку [Електронний ресурс] // Право і безпека. – 2011. – № 1. – Режим доступу: http://www.nbuv.gov.ua/portal/soc_gum/pib/2011_1/PB-1/PB-1_16.pdf*
8. *Лопашенко Н. Рейдерство / Н. Лопашенко // Законность. – 2007. – № 4. – С. 7-12*
9. *Рейдерство как социально-экономический и политический феномен современной России. Отчет о качественном социологическом исследовании. Исследование центра политических технологий 20.05.2008 //сайт Компромат.ру [Электронный ресурс]. Режим доступа: http://compromat.ru/main/mixl/raiderycpt.htm*
10. *Поняття рейдерства та його суспільна небезпечність [Електронний ресурс] // Юридична консультація в Інтернеті Pozov.com.ua. – Режим доступу : http://www.pozov.com.ua/ua/rejderstvo_ua.html*
11. *Симаков С. Рейдерство по-украински (краткий очерк) / С. Симаков // Юридичний радник. – 2006. – № 6 (14). – С. 23-25*
12. *Головань І. В. Рейдерство – модний термін чи зручна ширма? / І. В. Головань // Вісник господарського судочинства. – 2008. – № 6. – С. 125-128*
13. *Бєліков О. І. Рейдерство в Україні – реалії сьогодення / О. І. Бєліков // Юридичний журнал. – 2007. – № 4. – С. 105-109.*
14. *Полушкин О. А. Рейдерство: пути решения актуальных проблем / О. А. Полушкин // Закон и право. – 2008. – № 2. – С. 62-65*
15. *Варналій З., Мазур І. Основні передумови та шляхи подолання рейдерства в Україні. [Електронний ресурс] / З. Варналій, І. Мазур // Аналітична записка Національного інституту стратегічних досліджень – Офіційний сайт Національного інституту стратегічних досліджень. – Режим доступу: http://old.niss.gov.ua/Monitor/juli/1.htm*
16. *Економічна безпека підприємства в умовах рейдерських загроз: колективна монографія [Текст] / [О. А.Бурбело, С. К. Рамазанова, О. М. Заєць, Т. С. Гудіма, О. М. Кузьменко / за наук. ред. О. А. Бурбело, С. К. Рамазанова]. – Сєвєродонецьк: Вид-во СНУ ім. В. Даля, 2015. – 285 с.*

17. Бут Н. Д. Противодействие недружественным поглощениям / Н. Д. Бут // – Научно-практическое пособие. – М.: ОЛМА-ПРЕСС, 2006. – 352 с.
18. Ионцев М. Г. Корпоративные захваты: слияния, поглощения, гринмэйл / М. Г. Ионцев // – 2-е изд., перераб. и доп. – М. : Ось-89, 2006. – 224 с.
19. Федоров А. Ю. Рейдерство и корпоративный шантаж (организационно-правовые меры противодействия) : монография / А. Ю. Федоров // – М. : Волтерс Клувер, 2010. – 480 с.
20. Полушкин О. А. Экономическая преступность как фактор угрозы безопасности финансовой и хозяйственной деятельности предприятий / О. А. Полушкин // Закон и право. – 2005. – № 12. – С. 5-9
21. Гуман Е. О. Развитие организационно-экономического механизма защиты предпринимательской структуры от угрозы рейдерства : диссертация ... кандидата экономических наук : 08.00.05 / Гуман Екатерина Олеговна; [Место защиты : Ин-т экономики УрО РАН]. – Екатеринбург, 2010. – 277 с.
22. Мартынов С. Г. Гражданско-правовые механизмы защиты от недружественных поглощений хозяйственных обществ : диссертация ... кандидата юридических наук : / Мартынов Сергей Геннадьевич; [Место защиты: Российская академия народного хозяйства]. – Москва, 2011. – 173 с.
23. Берназ П. В. Рейдерство в Україні: визначення поняття / П. В. Берназ, О. О. Середа // Проблеми цивільного та господарського права. – 2008. – № 1. – С. 82-84.
24. Киреев А. Ю. Рейдерство в российской економике : сущность, тенденции и возможности противодействия : дис. ... канд. екон. наук : 08.00.05 «Экономика и управление народным хозяйством» / А. Ю. Киреев. — М., 2008. — 217 с.
25. Поняття рейдерства та його суспільна небезпечність [Електронне джерело] // Юридична консультація в інтернеті Pozov.com.ua. – Режим доступу : http://www.pozov.com.ua/ua/rejderstvo_ua.html.
26. Криничанский К. В. Рынок слияний и поглощений как среда реализации функции стимулирования предпринимателей и менеджеров / К. В. Криничанский //Менеджмент в России и за рубежом. – 2007. – № 3 – С. 115-118.
27. Борисов Ю. О. Корпоративное рейдерство как социально-экономическое явление в мировой экономике / Ю. О. Борисов. – М. : Первый ин-т корпоративного права, 2006. – 122 с.
28. Лазуренко В. И. Рейдерство : слияния и поглощения : монография / В. И. Лазуренко, Я. Н. Лоиакин, Ю. В. Лазуренко // – М. : ТУКБИ, 2009. – 232 с.
29. Понятие рейдерства. Факторы // Real Estate Development Group. – [Электронный ресурс]. Режим доступа: http://www.red-develop.com/ru/informaciya/analitika/115.html.
30. Гуторова Н. О. Щодо встановлення кримінальної відповідальності за рейдерство / Н. О. Гуторова // Юридичний радник. – 2007. – № 2. – С. 6-9.
31. Мігус І. П. Корпоративне управління в системі економічної безпеки акціонерних товариств України : Монографія / І. П. Мігус, Л. М. Худолій, М. П.Денисенко, С. П. Міхно. – Черкаси: ТОВ «Маклаут» – 2012. – 274 с.
32. Рейдеры атакуют универмаг «Украина» [Електронний ресурс]. – Режим доступу з екрану: http://narodna.pravda.com.ua/politics/4eb945efa397a/
33. В Ужгороді рейдери захопили готель «Закарпаття» [Електронний ресурс]. – Режим доступу з екрану: http://karpatnews.in.ua/news/31818-khto-stoit-za-reiderskoiu-atakoiu-na-naibilshyi-hotel-zakarpattia.htm
34. Молодецький С. С. Рейдерство як загроза економічній безпеці підприємств. Дис. канд. екон. наук: 21.04.02. – Режим доступу: https://drive.google.com/file/d/0Bz9Pblt6U8UmZ3ZUU2ZIcWlHUFk/view
35. Рейдерский захват предприятия: как противостоять [Электронный ресурс] / Название с титульного экрана: http://jupro.ru/reyderskiy_zahvat_predpriyatiya_kak_protivostoyat/

36. Бурбело С. О. Методи досягнення корпоративного контролю над підприємствами – об'єктами рейдерських атак [Електронний ресурс] / С. О. Бурбело // – Режим доступу: http://www.nbuv.gov.ua/old_jrn/Soc_Gum/VSUNU/2011_7_2/Burbelo.pdf
37. Молодецький С. С. Новітні форми рейдерства / С. С. Молодецький // Управління діяльністю суб'єктів господарювання в сучасних умовах: Матеріали Всеукраїнської науково – практичної заочної конференції, Черкаси, 30-31 травня 2013 р. / за ред. проф. Мігус І. П. – Черкаси: вид-во ПП Чабаненко Ю.А., 2013. – 68 с. – С. 63-65.
38. «Еенергоатом». Приватизаційна афера [Електронний ресурс]. – Режим доступу з екрану: http://www.zahvat.net/6/13384/
39. Молодецький С. С. Рейдерство у державному секторі економіки держави / С. С. Молодецький // Механізм регулювання міжнародних економічних відносин: XXVIII Міжнародна науково-практична конференція, (м. Київ, 13-14 грудня 2013 р.). У 2-х частинах. – К. : Аналітичний центр «Нова Економіка», 2013. ч. 1. – 120 с. – С. 102-105.
40. Офіційний сайт Державної служби статистики [Електронний ресурс]. – Режим доступу: http://www.ukrstat.gov.ua/
41. Офіційне інтернет-сайт Антирейдерського союзу підприємців України [Електронний ресурс]. – Режим доступу: http://antiraider.ua

1.3. КОНЦЕПТУАЛЬНІ ОСНОВИ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ

ЗАХАРОВ ОЛЕКСАНДР ІВАНОВИЧ, *к.е.н., професор,*
директор навчально-наукового
інституту менеджменту безпеки
Університету економіки та права «КРОК»

Сучасна світова економіка характеризується високим рівнем нестабільності і невизначеності процесів, які в ній відбуваються. Всі ці процеси роблять сильно впливають на стан національних економік. Це обумовлено,в першу чергу, їх відкритістю і високим рівнем інтегрованості в світову економіку. З одного боку, такий стан національних економік дає їм великі можливості для економічного розвитку, а з іншого, об'єктивно формує нові загрози економічній безпеці, викликані в першу чергу посиленням конкуренції з боку провідних світових виробників.

На діяльність вітчизняних підприємств впливають не тільки процеси глобалізації економіки. Не менш складні і не до кінця зрозумілі процеси євроінтеграції України. Безумовно, з одного боку вони дають нові можливості для розвитку вітчизняних підприємств і в цілому економіки України. І в той же час несуть серйозні загрози не тільки для їх успішної діяльності та економічної безпеки, а й самому існуванню через низьку конкурентоспроможність продуктів, що вони випускають.

Економічна безпека підприємства - це категорія, яка характеризує ступінь адекватності реального стану функціональних складових економіки підприємства (фінансів, технологій, технічного оснащення, персоналутаінших) параметрам, що забезпечує йогостабільну роботуіотримання запланованого прибутку [4].

Забезпечення економічної безпеки в сучасних умовах є пріоритетним завданням керівників підприємств і їх власників. Цю діяльність необхідно здійснювати з урахуванням ряду внутрішніх і зовнішніх факторів, які мають пряме і сильний вплив на діяльність вітчизняних підприємств.

До зовнішніх факторів, які значно впливають на стан економічної безпеки підприємств в даний час і здатні на неї впливати в найближчій і віддаленій перспективі відносяться:

▪Процеси глобалізації світової економіки. Це дуже складні і не завжди зрозумілі процеси. З одного боку, вони дають нові можливості для розвитку підприємств, через вільний вихід на світові ринки, а з іншого несуть серйозні загрози для їх економічної безпеки через посилення міжнародної економічної конкуренції.

▪Активні євро інтеграційні процеси, які з одного боку відкривають європейський ринок для українських виробників, а з іншого боку формують серйозні загрози для вітчизняних підприємств у зв'язку з об'єктивно взрастающей конкуренцією.

▪Кризовий стан вітчизняної економіки. Дуже складно розвивати бізнес в умовах нестабільної економіки, коли важко знайти надійних партнерів по веденню бізнесу, а найголовніше платоспроможних споживачів продукту, що випускається підприємством.

▪Високий рівень корупції. Головна небезпека корупції полягає в тому, що вона порушує всі закони і традиції ринкової економіки. Не дає в повній мірі реалізувати всі ті можливості, які вона дає для розвитку держави, економіки, підприємств і особистості. Одним з її негативних наслідків є те, що частка малого та середнього бізнесу в ВВП країни всього 5 відсотків і в той же час в розвинених країнах вона сягає 60 - 70 відсотків.

▪Високий рівень організованої злочинності в сфері економіки. Вітчизняним підприємствам доводиться здійснювати свою діяльність в умовах постійних загроз пов'язаних з рейдерськими захопленнями, замовних вбивств власників і керівників підприємств, діями недобросовісних чиновників, шахрайством та інших.

До внутрішніх факторів, які впливають на діяльність підприємств і їх економічну безпеку відносяться:

▪Система управління підприємствами. Від ефективності управління в значній мірі залежить їх успішна робота, розвиток і в кінцевому підсумку економічна безпека. І навпаки, помилки в управлінні можуть призвести не тільки до серйозних економічних втрат, а й до руйнування підприємств і втрати бізнесу. Ефективне управління дозволяє вибрати оптимальний напрямок ведення бізнесу, розробити правильну стратегію і успішно її реалізувати.

▪Персонал підприємства або іншими словами його людський капітал відіграє значну роль у забезпеченні стабільної роботи, розвитку і економічної безпеки. Від рівня кваліфікації, мотивації сумлінно і творчо працювати в значній мірі залежить успішне ведення бізнесу, розробка та впровадження інновацій і в кінцевому підсумку економічна безпека підприємств.

▪Технічне оснащення і технології підприємства. Від рівня технічної оснащеності і технологій в кінцевому підсумку залежить якість, собівартість і в кінцевому підсумку конкурентоспроможність випускається підприємством продукту. А значить і його економічна безпека.

▪Загальна організація, технологічна і трудова дисципліна. Ці фактори прямо впливають на ефективність виробничої діяльності, в тому числі на продуктивність праці і якість виробленого продукту. Він повинен містити інноваційні рішення, бути якісним, собівартість його повинна задовольняти економічні інтереси підприємства, а ціна - споживачів. Від якості і вартості продукту залежить його затребуваність на ринку і конкурентоспроможність.

▪Корпоративна культура. Людський капітал підприємства може бути реалізований повною мірою для розвитку бізнесу тільки в тому випадку якщо буде створена на підприємстві доброзичлива і комфортна для роботи атмосфера. Шанобливе ставлення до співробітників з боку керівників підприємства в поєднанні з продуманими заходами морального і матеріального заохочення здатне створити творчу обстановку і мотивувати персонал на сумлінне виконання своїх функціональних обов'язків.

▪Служба безпеки. Повинна стати основою системи економічної безпеки. Для цього вона повинна мати відповідну організаційну структуру, чітко

визначені функції і завдання, висококваліфікований персонал і сучасне технічне оснащення.

Сучасна система економічної безпеки вітчизняних підприємств повинна повною мірою і об'єктивно враховувати ці чинники. Традиційні підходи до побудови систем економічної безпеки в умовах нових реальностей в економіці не завжди можуть бути адекватними тим загрозам і ризикам, які в даний час формуються в економіці.

Забезпечення економічної безпеки підприємств України в період активізації євро інтеграційних процесів є пріоритетним завданням, як самого бізнесу, так і органів державної влади, які відповідають за національну економіку і її безпеку. Це обумовлено тим, що інтеграція в ЄС дасть не тільки нові можливості для розвитку економіки України, але створить серйозні загрози, пов'язані з високим рівнем конкуренції, в основі якої лежить висока якість товарів, що випускаються в країнах Європейського Союзу. У цих умовах успішна робота і розвиток українських підприємств в значній мірі залежить від здатності адаптуватися до стандартів європейського ринку. А це означає, що якість і ціна продукції, що випускається, повинні відповідати аналогічної продукції, що випускається підприємствами країн, входять до євро союз, а також тієї продукції, яка традиційно поставляється до єврозони провідними світовими виробниками з інших світових економічних центрів, в тому числі, з США, Китаю, Південної Кореї, Японії. Досягти успіху на європейському ринку можна тільки в тому випадку, якщо продукція українських підприємств зможе успішно конкурувати з продукцією провідних світових виробників. Це наслідок глобалізації світової економіки, яка створила умови для вільного переміщення товарів, послуг, фінансів і технологій. В результаті відбулося насичення європейського ринку високоякісними продуктами. І як наслідок такого розвитку світової економіки, серйозною проблемою для всіх товаровиробників стала жорстка міжнародна економічна конкуренція, яка загострила боротьбу за споживача продукції, що випускається в глобальному масштабі. Ситуація для вітчизняних підприємств ускладнюється ще й тим, що їм доводиться

здійснювати свою діяльність в умовах економічної кризи. В результаті на них сильно впливає значне число несприятливих факторів зовнішнього і внутрішнього середовища. Все це необхідно в повному обсязі враховувати при організації діяльності спрямованої на протидію загрозам економічної безпеки підприємств.

У цих умовах для того, щоб вітчизняні підприємства успішно працювали і не понесли економічні втрати в процесі входження в єврозону необхідно здійснити ряд серйозних підготовчих заходів.

Особливу увагу керівники підприємств повинні звернути на забезпечення економічної безпеки, як основу стійкої роботи і розвитку в умовах нестабільної економіки. З огляду на високий рівень невизначеності процесів протікають в економіці, а також багато векторний характер існуючих загроз, необхідно впроваджувати системний підхід для здійснення протидії їм. На основі впровадження інноваційних рішень необхідно створити ефективні, інтелектуальні системи економічної безпеки, здатні адекватно протидіяти існуючим та можливим загрозам зовнішнього і внутрішнього середовища підприємства.

Системний підхід передбачає розглядзабезпечення економічної безпеки підприємства як складний вид діяльності, що включає багато окремих напрямків, які пов'язані між собою і становлять єдине ціле. До основних напрямів діяльності системи економічної безпеки підприємств відноситься захист інформації, фінансів, території, виробничих і адміністративних будівель і споруд, засобів виробництва, готової продукції та сировини, комерційної таємниці та інтелектуальної власності, фінансів, транспортних засобів, персоналу.

Важливим напрямком в діяльності системи економічної безпеки має стати налагодження і постійна підтримка партнерських відносин з органами державної влади та правоохоронними органами України.

Особливу увагу в сучасних умовах система економічної безпеки повинна звертати на створення і підтримання сприятливих умов для ведення бізнесу

через налагодження взаємодії з органами державної влади, правоохоронними органами з метою протидії організованій злочинності у сфері економічної діяльності (корупції, рейдерських захоплень і т.д.) і підтримки партнерських відносин з суб'єктами недержавної системи безпеки. Успішна діяльність системи економічної безпеки по всіх перерахованих напрямках дозволить підприємству не тільки стабільно працювати в умовах економічної кризи, але може створити передумови для його розвитку. Тому сучасна система економічної безпеки підприємства складна як за структурою, так і за напрямками діяльності. Складність структури системи економічної безпеки зумовлена необхідністю використання всіх внутрішніх і зовнішніх ресурсів підприємств для протидії існуючим небезпекам і загрозам для їх діяльності в умовах нестабільної економіки. Без цього сучасним загрозам і небезпекам в сфері економіки протистояти практично неможливо. Для цього необхідно не тільки оптимально визначити всі необхідні ресурси, але що не менш важливо, створити правову базу для їх використання, а також ефективні механізми управління і взаємодії. Це обумовлено тим, що в період глобалізації економіки система економічної безпеки підприємств повинна протидіяти загрозам і небезпекам, які мають безліч різновидів, формуються в різних середовищах і відрізняються різним ступенем впливу на діяльність підприємства і його економічну безпеку. Для протидії цим загрозам необхідно використовувати всі внутрішні і зовнішні ресурси підприємства, а не тільки можливості його штатного підрозділу економічної безпеки. Системний підхід як раз і дозволяє це зробити.

В даний час серед вчених і практиків у сфері безпеки існують різні точки зору на зміст поняття «система економічної безпеки підприємства». З огляду на те, що в сучасних умовах забезпечити захист підприємств можливо лише за підтримки влади, слід розглядати систему економічної безпеки підприємств не з позиції використання для її побудови тільки їх внутрішніх ресурсів, а значно ширше виходячи за рамки власне підприємств.

Система економічної безпеки підприємства повинна мати чітку структуру, яка повинна включати всі внутрішні підрозділи підприємства, які можна задіяти з метою проведення заходів з комплексного протидії існуючим та можливим загрозам Всі елементи системи економічної безпеки повинні бути взаємопов'язані і координувати свою діяльність через механізм взаємодії. Врахоуючи те, що загрози для діяльності підприємства завжди існують і при цьому під впливом процесів, які відбуваються в економіці, постійно змінюються, система економічної безпеки підприємства повинна, по-перше, функціонувати постійно, а по-друге безперервно розвиватися, щоб адекватно протидіяти як існуючим так і новим небезпекам і загрозам.

Забезпечення економічної безпеки підприємства в сучасних умовах вимагає значних ресурсів, в тому числі адміністративних, правових, інтелектуальних, фінансових, матеріально-технічних та інших. У повному обсязі забезпечити всі потреби системи економічної безпеки складно, а точніше практично неможливо. Це означає, що в її діяльності повинні бути пріоритети. Система безпеки повинна здійснювати свою діяльність цілеспрямовано. Концентрувати свої зусилля на головних напрямках в першу чергу на тих, де формуються найбільш серйозні загрози для діяльності підприємства і його економічної безпеки. З огляду на високий рівень невизначеності процесів в економіці у системи економічної безпеки завжди повинні бути альтернативні напрямки діяльності та розвитку.

Система економічної безпеки підприємства в сучасних умовах може бути ефективною тільки в тому випадку, якщо буде включати дві підсистеми – внутрішню і зовнішню. Модель подібної системи економічної безпеки підприємства показана на рисунку 1.8.

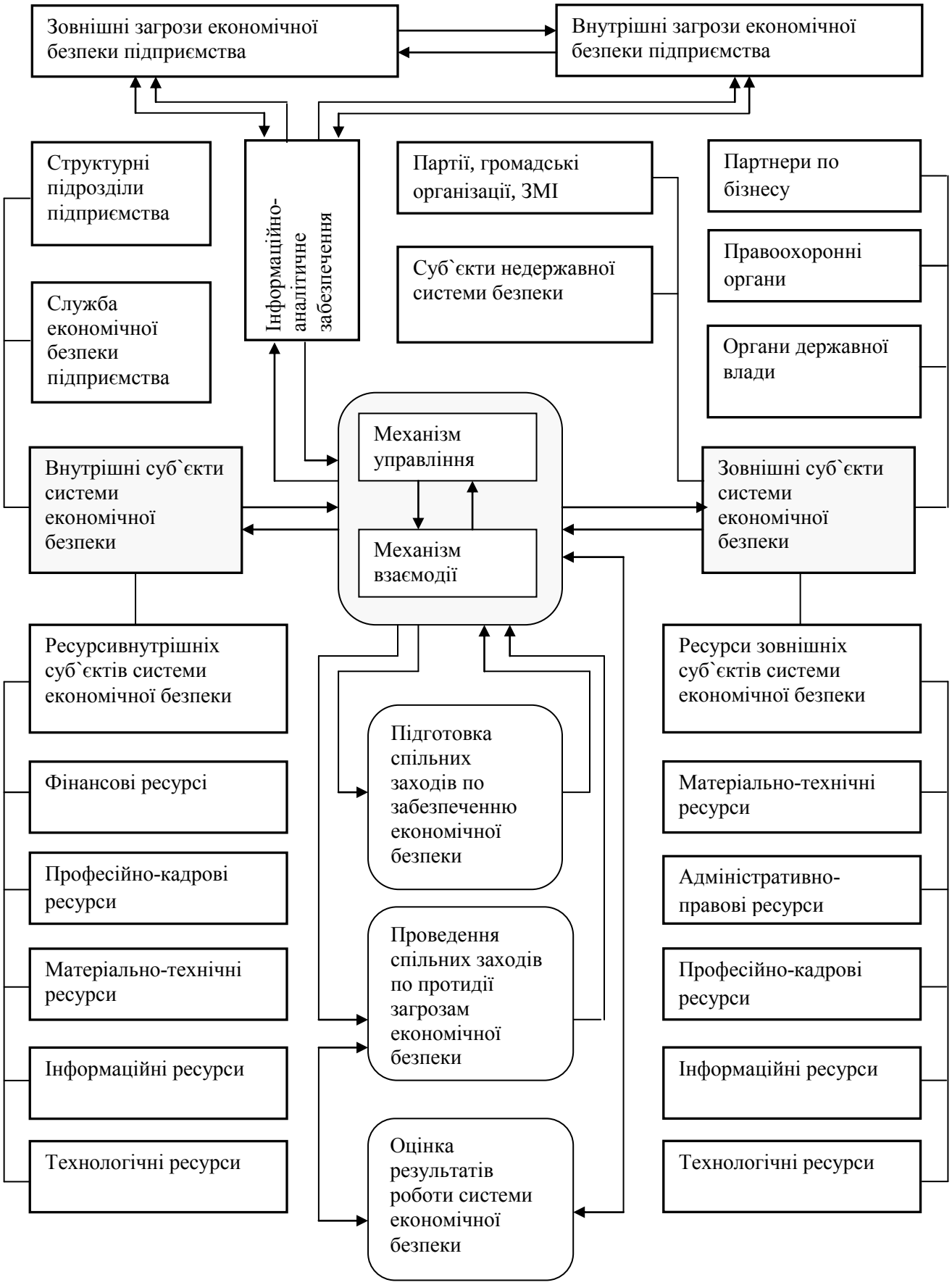


Рис. 1.8. Модель системи економічної безпеки підприємства

Джерело: розроблено автором

Даний підхід до побудови системи економічної безпеки підприємства дозволяє розглядати її як «сукупність внутрішніх і зовнішніхсуб'єктів забезпечення економічної безпеки підприємства, що мають спільні цілі, наділених відповідними функціями і правовими повноваженнями, що мають необхідну матеріально-технічну базу, підготовлений персонал, механізми управління і взаємодії, що володіють технологіями, формами і методами визначення, зниження рівня та протидії небезпекам і загрозам у сфері економіки» [4].

В якості внутрішньої підсистеми системи економічної безпеки підприємства слід розглядати всі його структурні підрозділи. Це дозволить використовувати для протидії небезпекам і загрозам економічної безпеки всі наявні на підприємстві ресурси, в тому числі фінансові, адміністративні, матеріально-технічні, інтелектуальні, правові та інші. І в першу чергу, в повній мірі задіяти для протидії факторам небезпек і загроз весь людський капітал підприємства - знання, вміння і навички всього персоналу, а не тільки співробітників штатного підрозділу економічної безпеки. Це дозволить ефективно протидіяти небезпекам і загрозам у всіх тих сферах, які впливають на діяльність підприємств. До цих сфер належать: правова, конкурентна, фінансова, взаємовідносин з органами влади та правоохоронними органами, техніко-технологічна, персоналу, взаємовідносин зі споживачами продуктів підприємства, інформаційна та інші.

Внутрішня підсистема є основою системи економічної безпеки підприємства. На неї покладаються основні завдання по створенню безпечних, сприятливих умов для стабільної роботи і розвитку підприємства. Рішення щодо створення системи економічної безпеки на підприємстві приймає його керівник або власник.

Формування вигляду внутрішньої підсистеми системи економічної безпеки залежить від ряду об'єктивних і суб'єктивних факторів в тому числі:

▪рівня існуючих загроз економічній безпеці підприємства і можливості появи нових, в найближчій і у віддаленій перспективі;

▪наявності на підприємстві необхідних ресурсів, які можна задіяти в системі економічної безпеки;

▪позиції керівників підприємства щодо того, якою має бути система економічної безпеки підприємства;

▪наявної законодавчої бази, яка регламентує діяльність у сфері безпеки;

▪наявності добре підготовлених фахівців в сфері безпеки.

При формуванні внутрішньої підсистеми системи економічної безпеки підприємства необхідно визначити:

▪основні завдання щодо забезпечення економічної безпеки, які буде вирішувати внутрішня підсистема системи економічної безпеки підприємства;

▪технології для протидії зовнішнім і внутрішнім небезпекам і загрозам економічної безпеки;

▪матеріально - технічні ресурси, які необхідні для ефективної діяльності з протидії зовнішнім і внутрішнім небезпекам і загрозам для діяльності підприємства;

▪структуру, функції, кількісно - якісні параметри персоналу, матеріально - технічне оснащення служби економічної безпеки підприємства, як головного структурного елементу системи економічної безпеки підприємства та його економічної безпеки;

▪визначити місце і роль кожного структурного підрозділу підприємства в системі його економічної безпеки;

▪механізми управління системою економічної безпеки;

▪механізми взаємодії служби економічної безпеки з іншими структурними підрозділами підприємства при підготовці і проведенні спільних заходів щодо забезпечення економічної безпеки;

▪інформаційно - аналітичне забезпечення діяльності, як всієї системи економічної безпеки, так і кожного окремого елемента системи;

▪визначити правові основи діяльності системи економічної безпеки підприємства.

В умовах глобалізації, економічної кризи і складних євро інтеграційних процесів особливу роль у створенні сприятливих умов для роботи вітчизняних підприємств відіграють зовнішні суб'єкти системи економічної безпеки. Їх умовно можна назвати зовнішньою підсистемою системи економічної безпеки підприємства.

Зовнішня підсистема системи економічної безпеки підприємства включає представників тих інститутів держави, які за своїм призначенням повинні забезпечувати економічну безпеку держави, а також суб'єкти недержавної системи безпеки, системи безпеки партнерів по бізнесу, суспільно-політичні організації, засоби масової інформації та незалежних журналістів, активістів громадянського суспільства. Головною метою зовнішньої підсистеми економічної безпеки є створення сприятливих умов для стабільної роботи, розвитку та забезпечення економічної безпеки вітчизняних підприємств.

Це обумовлено тим, що в умовах глобалізації та економічної кризи без підтримки держави вітчизняним підприємствам складно успішно здійснювати свою економічну діяльність як в середині країни, так і за її межами. Тому вся внутрішня і зовнішня політика держави має бути спрямована на підтримку вітчизняних товаровиробників. Усередині країни повинні бути створені всі умови для розвитку вітчизняного бізнесу. В першу чергу,малого і середнього.

Особливу роль в забезпеченні економічної безпеки підприємств відіграє економічний блок уряду, а також правоохоронні органи країни. Вони відповідають за створення і підтримання сприятливих і безпечних умов для ведення бізнесу. В поле їх діяльності знаходиться розробка і прийняття законів, які регулюють економічну діяльність в нашій країні. Не менш важливим напрямком в їх діяльності є створення умов, при яких закони, що регламентують економічну діяльність, дотримувалися всіма суб'єктами господарської діяльності, а також державними службовцями, які працюють в економічній сфері. В даний час найважливішими завданнями зовнішньої підсистеми системи економічної безпеки підприємства є боротьба з корупцією, яка представляє собою одну з найбільш серйозних загроз економічній безпеці

прямим наслідком, якої є викривлення законів ринкової економіки. В результаті звичайна конкуренція перетворюється в недобросовісну конкуренцію, в умовах якої не може успішно розвиватися малий і середній бізнес.

Без зовнішньої підсистеми системи економічної безпеки практично неможливо протидіяти організованій злочинності в економічній сфері. В першу чергу, це стосується захисту підприємств від рейдерських захоплень, а також організації протидії іншим злочинним технологіям, які використовують в даний час організовані злочинні угруповання. Ті, хто має на меті не тільки захоплення приватної власності, але також становлять загрозу життю і здоров'ю керівників підприємств, членам їх сімей, і персоналу підприємств.

В умовах глобалізації розвиток вітчизняних підприємств можливий лише за умови тісної їх взаємодії із зарубіжними партнерами,без яких неможливе технічне переоснащення підприємств, впровадження сучасних інноваційних технологій, і в підсумку успішний вихід зі своєю продукцією на закордонні ринки.

Зовнішньоекономічна діяльність в значній мірі залежить від роботи міністерства закордонних справ по створенню дружніх, партнерських відносин з зарубіжними країнами, в першу чергу, з тими, де українські підприємства здійснюють свою зовнішньоекономічну діяльність. Без створення режиму найбільшого сприяння для вітчизняного бізнесу складно здійснювати ефективну зовнішньоекономічну діяльність, а значить забезпечувати економічну безпеку, як держави, так і окремих підприємств.

В сучасних українських умовах органи державної влади мають досить великі можливості щодо забезпечення безпеки бізнесу. Особливо в таких сферах як протидія організованій злочинності, корупції, недобросовісної конкуренції, фінансових махінацій, інформації та інших. Дуже важливо забезпечити ефективну взаємодію органів державної влади та бізнесу в системі економічної безпеки підприємств. Для цього доцільно створити відповідні механізми і в першу чергу, механізм узгодження інтересів влади і бізнесу. В якості такого механізму можна розглядати«сукупність механізмів управління та

взаємодії, правових засад та принципів здійснення спільних дій, в рамках своїх повноважень, суб'єктів влади і бізнесу, спрямованих на створення сприятливих умов для стабільної роботи, розвитку та забезпечення економічної безпеки вітчизняних суб'єктів господарської діяльності»[5].

Важливою складовою зовнішньої підсистеми системи економічної безпеки підприємства являються його партнери по бізнесу. Це обумовлено тим, що вони об'єктивно зацікавлені в стабільній роботі підприємства, що дозволяє йому в повному обсязі і у встановлені терміни виконувати договірні зобов'язання. Підприємства - партнери також мають свої системи забезпечення економічної безпеки. Все це дозволяє здійснювати на основі взаємного інтересу взаємодію при проведенні заходів спрямованих на протидію несприятливим факторам, які несуть загрозу економічній безпеці підприємства. Взаємодія може бути у формі взаємного обміну інформацією про нові загрози для діяльності підприємств, надання допомоги в посиленні фізичного захисту підприємств для відображенні рейдерської атаки і т.д.

Особлива роль у зовнішній підсистемі системи економічної безпеки підприємств належить суб'єктам недержавної системи безпеки України. До них відносяться спеціалізовані підприємства, які надають послуги бізнесу в сфері безпеки. У тому числі, охоронні підприємства, які здійснюють на основі укладених договорв охорону об'єктів, вантажів, що перевозяться, а також забезпечують особисту безпеку власників підприємств і членів їх сімей. Підприємства, котрі займаются розробкою і випуском спеціальної техніки в тому числі засобів індівідуального захисту, сигналізації, відеоспостереження, фізичного захисту об'єктів, захисту інформації від несанкціонованного доступу, спеціального форменного одягу. А також консалтингові фірми, які надають інформаційні послуги в сфері безпеки бізнесу.

В умовах економічної кризи на діяльність вітчизняних підприємств постійно впливає значне число несприятливих факторів зовнішнього і внутрішнього середовища.

Всі їх необходимо враховуваті при організації діяльності системи економічної безпеки, щоб своєчасно і адекватно протидіяти. У цих умовах успішна діяльність із забезпечення економічної безпеки підприємства в значній мірі залежить від ефективності механізму управління. При прийнятті управлінських рішень в системі економічної безпеки підприємства необхідно враховувати значнукількістьфакторів загроз зовнішнього і внутрішнього середовища. При цьому особливу увагу слід приділяти процесам, які відбуваються у зовнішньому середовищі, тому що саме тут з одного боку знаходяться, нові можливості для розвитку підприємства, а з іншого боку формуються головні загрози його економічної безпеки.

В умовах економічної кризи загрози економічній безпеці підприємства формуються в різних сферах. Вони можуть надавати пряме чи непряме вплив на діяльність підприємства і його економічну безпеку. На рисунку 2 показана модель впливу факторів загроз зовнішнього середовища на економічну безпеку підприємства. Особливістю запропонованої моделі, є те, що вона розглядає не тільки зовнішнє середовище безпосередньо підприємства, але також пропонує розглядати зовнішнє середовище підприємств - партнерів та підприємств - конкурентів, де також можуть формуватися серйозні загрози для економічної безпеки підприємства.

Враховуючи те, що загроз економічній безпеці дуже багато, необхідно їх диференціювати. Для цього слід в першу чергу розділити їх на загрози прямої і непрямої дії. Це можливо зробити за умови глибокого моніторингу та аналізу процесів, які відбуваються у зовнішньому і внутрішньому середовищі підприємства.

Тільки виявлення, аналіз і оцінка існуючих загроз дозволить виділити ті з них, які здійснюють прямий негативний вплив на діяльність підприємств. Цим загрозам необхідно приділити особливу увагу з боку системи економічної безпеки підприємства. Слід пам'ятати, що у кожного підприємства є своє зовнішнє середовище, а в ній можливості і загрози для діяльності підприємства.

Тому представлену на рисунку 1.9 модель впливу факторів загроз зовнішнього середовища на економічну безпеку підприємства слід розглядати як чисто теоретичну, і яка не має відношення до конкретного підприємства.

При вивченні зовнішнього середовища необхідно приділяти увагу не тільки процесам, які відбуваються безпосередньо навколо підприємства. Слід також звернути пильну увагу на те, що відбувається у зовнішньому середовищі підприємств - партнерів та підприємств - конкурентів. Це обумовлено тим, що при сприятливому розвитку процесів у зовнішньому середовищі підприємств - партнерів вони зміцнюють свої позиції на ринку і підвищують свою економічну безпеку. У цьому випадку ступінь їх надійності зростає, і вони не несуть загрозу економічній безпеці підприємства через невиконання своїх договірних зобов'язань. І навпаки, якщо в зовнішньому середовищі підприємств - партнерів відбуваються несприятливі процеси, негативно впливають і здатні вплинути на їх економічну діяльність, то в цьому випадку виникає загроза невиконання або неповного виконання підприємствами-партнерами своїх договірних зобов'язань. В цьому випадку об'єктивно виникає загроза збою в роботі підприємства, а це означає появу загрози його економічній безпеці.

Такий же підхід доцільно застосувати і щодо оцінки зовнішнього середовища підприємств-конкурентів. У цьому випадку все слід оцінювати навпаки. Якщо при вивченні зовнішнього середовища підприємств - конкурентів виявляються сприятливі для їх діяльності чинники, то можна припустити, що вони будуть розвиватися і підвищувати свою конкурентоспроможність, а значить нести пряму загрозу економічній безпеці підприємства через пропозицію більш привабливих для споживачів продуктів або послуг. І навпаки, якщо у зовнішньому середовищі підприємств-конкурентів виникають несприятливі для їх діяльності чинники, то можна припустити, що під їх впливом підприємства - конкуренти знизятьтемпи свого розвитку і конкурентоспроможність. А це означає, що стануть представляти меншу небезпеку для підприємства.

Рис. 1.9. Модель впливу факторів загроз зовнішнього середовищана економічну бекзпеку підприємства

Джерело: розроблено автором

Ось для чого необхідно вивчати не тільки зовнішнє середовище підприємства, а також зовнішнє середовище підприємств - партнерів та підприємств - конкурентів. Без цього повної та об'єктивної інформації про

існуючі та можливі загрози для діяльності підприємства і його економічної безпеки, необхідної для прийняття управлінських рішень в системі економічної безпеки підприємства, не отримати.

Проведення постійного моніторингу зовнішнього і внутрішнього середовища підприємства з метою виявлення та ідентифікації небезпек і загроз економічній безпеці підприємств, а також прогнозування їх можливого розвитку і визначення можливого збитку, який вони можуть завдати економіці підприємств є одним з найбільш важливих і складних завдань системи економічної безпеки,без успішного вирішення якого неможливо створити ефективні механізми управління діяльністю системи економічної безпеки.

Керівникам підприємств для прийняття правильних рішень по веденню бізнесу та забезпечення його безпеки, перш за все, потрібна об'єктивна і максимально повна інформація про процеси, що відбуваються на ринку, і в першу чергу в тих його сегментах, де працює підприємство. Тому постійний пошук інформації необхідної для прийняття правильних управлінських рішень на стратегічному та оперативному рівнях, є однією з пріоритетних задач системи економічної безпеки підприємств. Успішне її рішення дозволить керівникам і провідним фахівцям підприємств не тільки розробити хорошу стратегію економічної безпеки, але і забезпечити успішну її реалізацію в процесі ефективного оперативного управління діяльністю всіх суб'єктів системи економічної безпеки.

Це можливо здійснити тільки при наявності в системі економічної безпеки високопрофесійного спеціалізованого підрозділу інформаційно-аналітичного забезпечення. Даний підрозділ може входити до складу служби економічної безпеки підприємств або бути окремим його структурним підрозділом, який безпосередньо підпорядковується керівнику підприємства.

Основним призначенням даного підрозділу є своєчасне забезпечення керівників підприємства та його системи економічної безпеки достовірною інформацією про процеси, які відбуваються у зовнішньому і внутрішньому середовищі. Це стосується визначення нових напрямків для розвитку бізнесу, а

також своєчасне виявлення нових і трансформацію існуючих загроз для його економічної безпеки. Дана інформація необхідна для прийняття правильних рішень на стратегічному та оперативному рівні управління підприємством.

На інформаційно-аналітичний підрозділ підприємства покладається рішення наступних завдань:

- здійснення постійного моніторингу процесів, що відбуваються у зовнішньому і внутрішньому середовищі підприємств;
- своєчасне виявлення, аналіз і оцінка сприятливих факторів для діяльності підприємств;
- своєчасне виявлення, аналіз і оцінка несприятливих чинників для діяльності підприємств;
- вивчення та прогнозування дій конкурентів;
- вивчення та прогнозування поведінки партнерів;
- вивчення поведінки споживачів продукції підприємств і прогнозування можливих змін їх переваг;
- вивчення, аналіз і прогнозування змін у внутрішній політиці держави;
- вивчення, аналіз і прогнозування розвитку зовнішньополітичної діяльності держави стосовно тих країн, де підприємства здійснюють свою зовнішньоекономічну діяльність;
- виявлення, вивчення і оцінка інноваційних продуктів того сегмента економіки в якому працює підприємство;
- виявлення і оцінка інноваційних технологій, матеріалів відповідають профілю діяльності підприємств;
- вивчення процесів, які відбуваються в світовій економіці і визначення ступеня їх загрози для того сегмента економіки де працюють підприємства та інших.

З огляду на, що на інформаційно - аналітичний підрозділ покладається вирішення складних завдань, пов'язаних з пошуком і систематизацією та аналізом інформації в умовах високої невизначеності процесів, які відбуваються в суспільстві, економіці і політиці в його складі повинні бути

висококваліфіковані аналітики та фахівці в галузі конкурентної розвідки. Крім цього рішення задач пов'язаних з вивченням ринку і дій конкурентів доцільно залучати маркетологів підприємства.

В умовах економічної кризи для забезпечення успішної діяльності вітчизняних підприємств необхідно створювати такі системи економічної безпеки, які зможуть забезпечити комплексну протидію всім існуючим і можливим загрозам зовнішнього і внутрішнього середовища.

Сучасні системи економічної безпеки повинні використовувати всі власні ресурси підприємств, а також ресурси зовнішніх організацій, які необхідно розглядати як зовнішні суб'єкти систем економічної безпеки підприємств. До зовнішніх суб'єктів системи економічної безпеки слід відносити, в першу чергу, органи державної влади та правоохоронні органи, які за своїм функціональним призначенням несуть пряму відповідальність за забезпечення національної безпеки в сфері економіки. Необхідно в системі економічної безпеки в повній мірі задіяти також можливості суб'єктів недержавної системи безпеки України, в тому числі охоронних підприємств, служб безпеки партнерів по бізнесу, консалтингових фірм в сфері безпеки, підприємств, які виробляють технічні засоби забезпечення безпеки та інших.

Для того, щоб отримати синергетичний ефект в системі економічної безпеки підприємства, необхідно особливу увагу звернути на створення в системі управління ефективного механізму взаємодії, за допомогою якого можна скоординувати підготовку, всебічне забезпечення і своєчасне проведення спільних заходів з протидії загрозам для діяльності підприємства і його економічної безпеки.

Список використаних джерел:

1. *Економічна безпека суб’єктів господарської діяльності в умовах глобальної фінансової кризи. Монографія. / Кириченко О.А., Захаров О.І., Денисенко М.П. та ін. // К.: ТОВ "Дорадо-Друк" – 2010. – 412 с.*
2. *Система економічної безпеки: держава, регіон, підприємство. Монографія. / Козаченко Г.В., Захаров О.І., Ляшко О.М. та ін.// Луганск: Видавництво Східноукраїнського національного університету. 2011.- 284 с.*
3. *Теоретико-методологические и прикладные основы обеспечения экономической*

безопасности субъектов хозяйственной деятельности. Монографія. / Захаров О.І., Пригунов П.Я., Гнилицкая Л.В. // К.: ТОВ «Дорадо-Друк», 2011. – 290 с.

4. Захаров О.І. Теоретичні основи забезпечення економічної безпеки підприємств /Захаров О.І.// Вчені записки університету «КРОК», – 2012.- № 31. – С. 80- 88.

5. Захаров О.І. Механізм взаємодії влади та бізнесу в системі економічної безпеки /Захаров О.І.// Черкаси: Збірник наукових праць Черкаського державного технологічного університету (Економічні науки), випуск 12, частина 3. 2015. - 150 с.

6. Захаров О.І. Синергетичний ефект в системі економічної безпеки підприємства /Захаров О.І.// Черкаси: Збірник наукових праць Черкаського державного технологічного університету (Економічні науки), випуск №1. - 2016. - 151 с.

7. Козаченко Г.В., Пономарьов В.П., Ляшенко О.М. Економічна безпека підприємства: сутність та механізм забезпечення: монографія / Г.В. Козаченко, В.П. Пономарьов, О.М. Ляшенко - К: Лібра, 2003. - 280с.

8. Шлыков В. В. Комплексное обеспечение экономической безопасности предприятия. – СПб: "Алетейя" 1999.-144с.

9. Шемаєва Л. Г. Економічна безпека у стратегічній взаємодії з суб'єктами зовнішнього середовища : автореф. дис. на здобуття наук. ступеня д-ра екон. наук: спец. 21. 04. 02 / Л. Г. Шемаєва. – К., 2010. – 39 с.

10. Ярочкин В. И. Система безопасности фирмы / В. И. Ярочкин. – М. : Ось-89, 2003. – 352 с.

1.4. THE COMPARISON OF ECONOMIC CRIME LEVEL IN SELECTED EUROPEAN COUNTRIES USING THE ZERO UNITARIZATION METHOD

DOMAŃSKA A., *M.Sc, Research-and-teaching Assistant*
Department of Banking, Maria Sklodowska Curie University in Lublin
LEWICKA B.A., *M.Sc, Research-and-teaching Assistant*
Department of Banking, Maria Sklodowska Curie University in Lublin

Introduction. The level of economic crime is an issue of ever-growing concern all around the world. According to the Global Economic Crime Survey 2016 regularly conducted by PwC, 36% of examined companies claimed that they have been affected by at least one incident of economic crime in the past two months[1]. The most worrying fact is that methods of committing an economy crime are becoming more diverse and protection mechanisms seem to be insufficient. The best example is the widespread of cybercrime activities, which are the second most popular crime which respondent companies have been experienced.The variety of possible cyberattacks requires from companies proper compliance programmes and ICT (Information and Communication Technologies) security policy, which have not been implemented in many enterprises yet.

The main goal of this paper is to evaluate the level of economic crime for selected European countries, taking under consideration accessible indicators such as the widespread of criminal incidents, opinions about local law effectiveness and popularity of protection mechanisms across enterprises. In order to standardise the results and give them ranking positions, the statistical zero unitarization method was applied. This approach can become useful in case of preparing trustworthycross-country comparisons.

Moreover, hypothesis stated in this article is that having formal business ethics and compliance policy does not ensure sufficient protection against economic crime.

Methods and materials. This article compares the level of economic crime in selected countries. In order to estimate this level we based on quantitative secondary

[1] PwC, Global Economic Crime Survey 2016, www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

data(in form of accessible indicators). Most of the data comesfrom territory reports based on research entitled "Global Economic Crime Survey 2016" which are conducted by the global audit firm PwC (PricewaterhouseCoopers International) every second year. The research was carried out among the highest-level executives in senior management (c-suite) and heads of departments or business units in 115 countries in 17 different languages. In total, more than 6300 surveys were completed[2]. Nevertheless, not all participating countries are discussed in this article. The choice of analysed countries was mostly determined by data accessibility and limited only to European region. Additional indicators were found in the Eurostat database[3].

The strengths of those sources are data reliability, completeness and fact that they can ensure the high level of comparability. The significant weaknesses are delays in publishing and lack of specific information for some countries.

In order to estimate the level of economic crime in those countries and rank them correctly, the zero unitarization method was applied. This normalisation method was chosen, because it is applicable with both quantitative and qualitative variables[4] and its simplicity leads to easy interpretation of gained results. Moreover, as Kukula states[5], this method fulfil three important criteria:

1. After normalisation lengths of intervals of variability for all features are the same.

2. The lower and upper limits of intervals of variability for all features are the same: [0,1].

3. Features which have a zero value can be also normalised.

Below we present formulas used in zero unitarization method[6]:

$$z_{ij} = \frac{x_{ij} - \min_i x_{ij}}{\max_i x_{ij} - \min_i x_{ij}}, X_j \in S \quad (1)$$

[2]www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html (30.03.2016).
[3] Eurostat, www.ec.europa.eu/eurostat (30.03.2016).
[4] Kukuła K., *Propozycja budowy rankingu obiektów z wykorzystaniem cech ilościowych oraz jakościowych*, „QuantitativeMethods In Economics", Vol. XIII, No. 1, Warsaw 2012, pp. 5-16.
[5]Ibidem.
[6]Kukuła K., Bogocz D., *Zero Unitarization Method And Its Application In Ranking Research In Agriculture, Economic and Regional Studies*, Volume 7, No. 3, 2014, pp 5-13.

$$z_{ij} = \frac{\max_i x_{ij} - x_{ij}}{\max_i x_{ij} - \min_i x_{ij}}, X_j \in D \quad (2)$$

Where: z_{ij} is the standardized value of the variable X_j in the object W_i and $x_{ij}$is the value of the variable X_j in the object W_i.

The object W_i is described by the vector of diagnostic variables:

$$X_i=[x_{i1}, x_{i2} \ldots x_{in}], (i=1, \ldots, r) \quad (3)$$

Formula 1 is used with variables which are stimulants (their increase causes higher level of analysed phenomena) and formula 2 is used with destimulants (if it increases, the value of analysed phenomena decreases).

In order to rank analysed countries, all variables need to be normalised and then summed up for each object[7]:

$$q_i = \sum_{j-1}^{n} z_{ij}, \quad i = (1, \ldots, r) \quad (4)$$

q_i - a synthetic variable, which assess the i-th object.

In case of this research, objects (W) are selected countries presented in the table 1. While diagnostic variables (X_i) – both stimulants and destimulants - are listed in the table 2 and described below. The analysed phenomenon is the level of economic crime in selected countries.

Table 1.1

The list of analysed objects (countries)

W_i	Country
W_1	Belgium
W_2	Cyprus
W_3	France
W_4	Luxemburg
W_5	Netherlands
W_6	Poland
W_7	Sweden
W_8	United Kingdom

Source: ownelaboration.

[7] Kukuła K., Bogocz D., *op. cit.*, p 7.

Table 1.2

The list of diagnostic features – stimulants and destimulants with the source and the data year

X_j	Feature	Source	Data year
Stimulants			
X_1	The percentage of companies which have experienced at least one incident of economic crime in the past 24 months	PwC Global Economic Crime Survey	2016
X_2	The percentage of companies which do not have confidence in state law enforcement against economic crime		
X_3	The percentage of companies which have experienced cybercrime in the past 24 months		
Destimulants			
X_4	The percentage of companies which have a formal business ethics & compliance programme	PwC Global Economic Crime Survey	2016
X_5	The percentage of companies which have the ICT security policy addressed the risks of destruction or corruption of data due to an attack or by unexpected incident	Eurostat	2015

Source: ownelaboration.

X_1 –The percentage of companies which have experienced at least one incident of economic crime is an indicator which shows how many respondent companies have noticed any type of economic crime (such as: asset misappropriation, cybercrime, bribery, corruption, procurement fraud, accounting fraud, money laundering etc.) in past 24 months. However, this indicator describes only those incidents which have been discovered (10% by accident)[8], so it can be assumed that the real number of committed crimes could be higher.

X_2–The percentage of companies which do not have confidence in state law enforcement against economic crime is an indicator which represents the companies perception of law enforcement quality (is it well-prepared to investigate and punish for economic embezzlements and is it properly resourced). Generally, this feature shows the level of trust in effectiveness of legal enforcement agencies.

[8]PwC, Global Economic Crime Survey 2016, *op. cit.*, p. 8.

X_3 - The percentage of companies which have experienced cybercrime in the past 24 months shows how many companies have been affected by a crime committed using the computer and internet. Examples of such offences are: viruses distribution, illegal file downloads, phishing (impersonating a trusted third party to gain access to private data[9]) pharming (secretly installing virus or malicious programme which takes user to an imitation of the legitimate site in order to steal personal information[10]) and other form of theft of personal information or intellectual property.

X_4–The percentage of companies which have a formal business ethics & compliance programme represents the percentage of firms that have claimed to have a formal regulations how to avoid the risk of economic crime incidents. Nevertheless, this indicator does not show the level of employees awareness of compliance policy and formal ethics.

X_5 - Percentage of companies which have the ICT security policy addressed the risks of destruction or corruption of data due to an attack or by unexpected incident. This indicator presents the preparation of non-financial enterprises, who employ more than 10 people, to protect themselves against cybercrime and its consequences.

In order to explain which of presented factors have the strongest relationship with the synthetic variables qi (calculated for all selected countries), the Pearson correlation analysis was carried out.Below, the applied formula for the Pearson correlation coefficient is presented and described[11]:

$$r_{qx_j} = \frac{\sum_1^n (x_{ij} - \overline{x_j})(q_i - \bar{q})}{\sqrt{\sum_1^n (x_j - \overline{x_j})^2 \sum_1^n (q_i - \bar{q})^2}}, \quad (5)$$

where:

r_{qx_j}– the correlation coefficient between the synthetic variables q_i for selected countries (objects W_i) and the values of the featureXj,

x_{ij} -the value of the variable $X_j$in the object W_i,

[9] Whittaker, C., Ryner, B., Nazif, M., Large-Scale Automatic Classification of Phishing Pages. In NDSS (Vol. 10), 2010, February.

[10] Brody R.G., Mulig E., Kimball V., Phishing, pharming and identity theft, Academy of Accounting and Financial Studies Journal 11 (3), 43, 2007.

[11] Sobczyk M., *Statystyka – aspekty praktyczne i teoretyczne*, UMCS, Lublin 2006, p. 161.

$\bar{x}_j$– - the mean value of the variable X_j,

q_i - the synthetic variable, which assess the i-th object,

$\bar{q}$ - the mean synthetic variable for all objects.

The interpretation of the correlation coefficient is as follow:[12]

•-1 - a perfect negative(downhill) linear relationship,

•more than -1 and less than -0,80- a very strong negative(downhill) linear relationship,

•more than -0,80 and less than –0,60 – a strong negative(downhill) relationship,

•more than -0,60 and less than –0,40 - a moderate negative (downhill) linear relationship,

•more than -0,40 and less than –0,20 – a weak negative (downhill) linear relationship,

•more than -0,20 and less than 0 - a very weak negative (downhill) linear relationship,

•0 - no linear relationship,

•more than 0 and less than 0,20 - a very weak positive (uphill) linear relationship,

•more than 0,20 and less than 0,40 – a weak positive(uphill) relationship,

•more than 0,40 and less than 0,60 - a moderate positive (uphill) linear relationship,

•more than 0,60 and less than 0,80 – a strong positive (uphill) relationship,

•more than 0,80 and less than 1 – a very strong positive (uphill) relationship,

•1 – a perfect positive (uphill) linear relationship.

Results. As the Global Economic Crime Survey shows, in 2016, 36% of all respondent companies declarethat they have been a victim of an economic fraud. It is one percentage point lower than in 2014 (figure 1). It is worth mentioning that 10 years ago,we noticed the significant decline in economic crime rate. In 2005 almost half of respondents (45%) claimed to had experienced this kind of offence in past 24

[12]Ibidem.

months. Today,10 percent less companies have a contact with thisthreat. Undoubtedly, this can be described as asignificant improvement. Still, we have to rememberthat some enterprises might have not noticed that they were the victim of the crime, especially cybercrime. This means that the statistics may actually be worse.

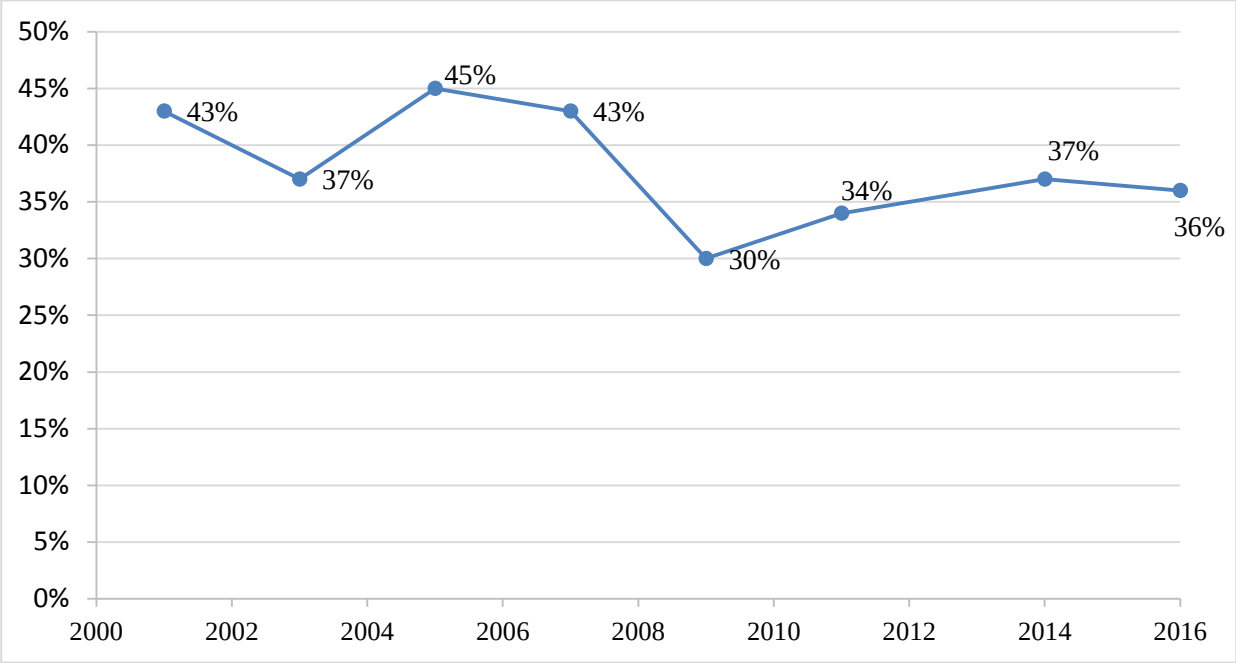


Figure 1.10. Reported rate of economic crime in respondent companies

Source: Global Economic Crime Survey 2016.

Furthermore, analysing the data in detail, it becomes visible, that rate of economic crime varies significantly between regions. The most experienced regions are Africa (57%), Western Europe (40%) and North America (37%). It should be highlighted that in case of Western Europe, economic crime level has risen sharply from 35% in year 2014. This substantial increase was caused mainly because of growing number of cybercrime incidents, especially in France and the United Kingdom. Whatsoever, situation of Eastern Europe has improved - in 2014, 39% of companies reported to have been experienced by economic crime.Today, according to this year research, the percentage of organisations affected by embezzlement is 6 percentage points lower. In conclusion, regions with a predominance of emerging markets have improved their situation. This might have been caused by implemented

improvements intheir legal systemsor by increasing companies' knowledge about the possible risks. Nevertheless, the situation of regions with more developed countries haveworsened, which is a worrying signal.

Table 1.3

Reported economic crime in 2014 and 2016

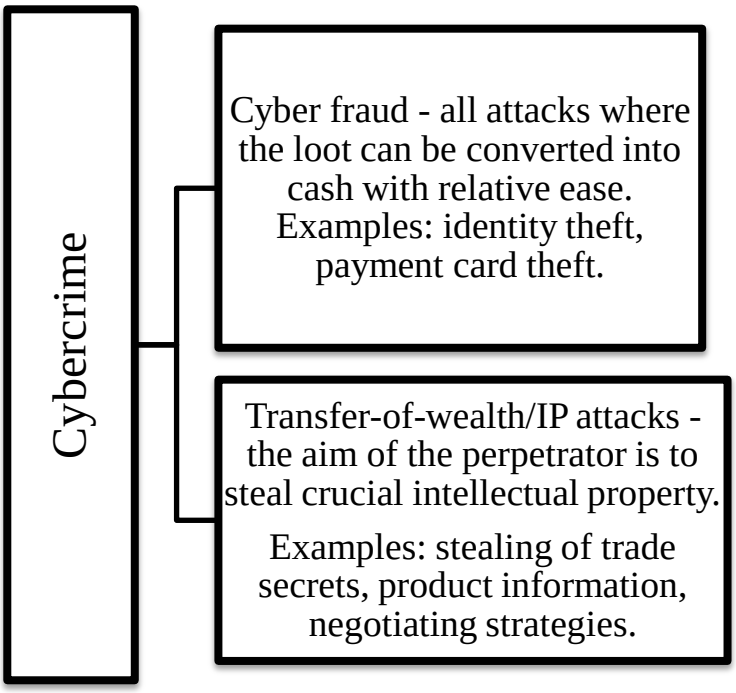
Region	Reported economic crime in 2016	Reported economic crime in 2014
Africa	57%	50%
Western Europe	40%	35%
North America	37%	41%
Eastern Europe	33%	39%
Asia Pacific	30%	32%
Latin America	28%	35%
Middle East	25%	21%
Global	36%	37%

Source: Global Economic Crime Survey 2016.

A person who commits a crime may be as well a company employee as well as an external actor. In 46% cases it is an internal perpetrator, most frequently –a senior or middle manager. A typical offender is a male, between 31-40 years old, educated, who has served for company for from 3 to 5 years. Nevertheless, the survey reveals that in European countries, crime incidents were more often committed by external actors. Globally, the most common frauds have been: asset misappropriation (62%)cybercrime (32%) and bribery and corruption (24%).

Among those three, cybercrime seems to be the most dangerous and difficult to hinder. It is a complex phenomenon, because it can be committed in many ways, and its consequences can be devastating not only for a company but also for its stakeholders (clients, providers etc.). We can distinguish two types of cybercrime: the first, connected only with stealing money and destroying company reputation and the second, far more dangerous – stealing enterprise's intellectual property. As the first obviously can generate high losses, the second may directly lead to company destruction if its know-how is uncovered[13].

[13] PwC, Global Economic Crime Survey 2016, *op. cit.*, p. 19



Scheme 1. Two main categories of cybercrime with examples

Source: own elaboration based on Global Economic Crime Survey 2016, p. 19.

But what is the most important, this threat is becoming more widespread due to the growing popularity of the ICT. As the Global Economic Crime Survey presents, in two years the number of cybercrime incidents has already tripled. What is more, actually all industries are at risk. Even if they considered themselves as unlikely targets in the past. According to PwC's Global State of Information Security Survey 2016, the sector registering the most significant increase in cybercrime activity in 2015 was retail, while financial services – still one of the most attacked sectors – had levelled out, with very little growth in terms of number of attacks over the last three years.[14]

Moreover, a worrying fact is that nearly 44% of all survey respondents, are not sure that their local law enforcement agencies are adequately prepared to defend them against economic crime, 28% of respondent do not know if they are properly trained and resourced. Hence, creating more effective self-defence mechanisms inside companies seems to be justified.

[14]PwC, Global Economic Crime Survey 2016, *op. cit*., p. 18.

As an example of such a mechanism may serve a formal business ethics & compliance programme, which 82% of companies claim to have. Nevertheless, 20% of respondents are not aware of it. The Global Economic Crime Survey reveals that there is a significant gap in perception of organisational values between senior and middle management. This situation gives rise to problems with an effective implementation of policy into practice.

However, regarding to escalating danger of cybercrime, a general compliance programme may seem to become insufficient. Hence, the ICT security policy addressed the risks of destruction or corruption of data is a compulsory must-have for all enterprises. Unfortunately, as the Eurostat has estimated, in the European Union only 28% of companies who employ more than 10 people (apart from financial sector) have this self-defence mechanism introduced.

According to the standardized data, it seems to be clear that the biggest problem in Belgium, in comparison to other countries, is cybercrime experienced by companies.This is a big threat for their functioning. Although more and more enterprises acknowledge the risk of cyber threats, still many of them have failed to prevent cyber-attacks in the past 24 months.Digital technology continues to transform and disrupt the world of business, exposing organizations to both: opportunities and threats. So it is hardly surprising that 52% of Belgian companies have experienced cybercrime in past 2 years. This implicates onthe high rate of experience of economic crime, which means that it is an obstinate threat to businesses in Belgium, with about half (45%) of organizations experiencing someform of it in the past 24 months.In addition, the Belgians still have a small degree of trust in legal system.This means that companies are left to themselves in the fight against economic crime. Results show that the complexity of economic crime and the role that technology plays in its evolution is becoming higher. This is hardly a surprise in a business environment characterized by growing globalization that vigilant enforcement increases and greater public accountability is demanded. When the state policy fails, it is a company obligation to identify and mitigate risks.

Table 1.4

Economic crime in Belgium

X_j	Features	Data	Normalized data
X_1	Experience of economic crime	45%	0,44
X_2	Low confidence in law enforcement	44%	0,48
X_3	Experience of cybercrime	52%	0,78
X_4	Formal business ethics & compliance programme	82%	0,25
X_5	The ICT security policy	30%	0,33
Sum		x	2,28

Source: own estimations based on Global Economic Crime Survey 2016 and Eurostat data.

However, in France, the situation is even worse.Among all analysed countriesFrance has fared the worst in the experience of economic crime (especially cybercrime). Up to 61% of the surveyed companies have been affected by thisoffence. It means that most companies are still not adequately prepared for (or even do not understand) all potential risks. Using virtual toolswithout adequate protection – this is the issue why somany French organizations are so prone to cyber-attacks. However, this problem derives from such defaults as: the board's underappreciation of the risks, insufficient controls under third party vendors with access to the organization's technology environment (especially in the context of increased outsourcing) and inadequate cyberresponse plans.What is more, French companies still do not believe in the effectiveness of the state and policein prevention and detectionof such crimes. It is interesting that the respondentshave a good opinion about themselves and their formal business ethics and compliance programme. It is possible that the problem lies not onlyin the authorities and inadequate enforcement tools but also in the companies themselves and their ineffectiveprogrammes.

Conversely, in the Netherlands the biggest problem is a low percentage of companies which have formal business ethics and compliance programme (71%). Although Dutch companies reportquite low level of incidences of fraud in comparison to the other countries,it is still higher than the global average. A little less than a half (45%) of companies have experienced economic crime in past 24 months.

Table 1.5

Economic crime in France

X_j	Features	Data	Normalized data
X_1	Experience of economic crime	68%	1,00
X_2	Low confidence in law enforcement	51%	0,74
X_3	Experience of cybercrime	61%	1,00
X_4	Formal business ethics & compliance programme	84%	0,13
X_5	The ICT security policy	24%	0,56
Sum		x	3,42

Source: own estimations based on Global Economic Crime Survey 2016 and Eurostat data.

Cybercrime incidents also have occurred frequently. But, despite the fact that this threat it is a matter of great concern for many organisations, some of them still do not have a fully operational incident response plan to deal with it. Many organisations have been cutting costs in bothheadcount and training, or stretching their existing team'sresponsibilities to include additional duties. This kind of approach may lead to astrategic miscalculation. Moreover, it should be highlighted that the insidious nature of cybercrimemeans that companies which claim not to be victims, may as well be not aware of it. A concerning trend we have observed isthat hackers manage to remain on organisations'networks for extended periods of time without being detected.So it is likely that the actual number of crimes is higher.

Table 1.6

Economic crime in Netherlands

X_j	Features	Data	Normalized data
X_1	Experience of economic crime	45%	0,44
X_2	Low confidence in law enforcement	49%	0,67
X_3	Experience of cybercrime	42%	0,54
X_4	Formal business ethics & compliance programme	71%	0,94
X_5	The ICT security policy	24%	0,56
Sum		x	3,14

Source: own estimations based on Global Economic Crime Survey 2016 and Eurostat data.

In contrast, a low belief in the law in Luxembourg does not correlate with a high crime rate. About 46% of entrepreneurs do not trust the authorities. They believe that law will not protect them sufficiently. But in the reality, in comparison to other states, the factor of experience of economic crime is relatively low. Only about quarter (24%) of organisations have been affected by cybercrime in the past 24 months. This is due to thefact that more organisations in Luxembourg leave thefirst response to their IT teams which are supported by senior management and other key players.

What is more, the composition of these response teams is often better educated, which ultimately affects the handlingof breaches.This means that thesecrimes becoming easierto detect or companies are simply becoming more aware of changing threats that every business faces. Possibly, companies evaluate and potentially reimagine the identity ofcompliance function so it may adapt to an environment where risk and threats are ever-changing. Nevertheless, policies and training on values are not enough. Essential is thecredible, consistent engagement across the organisation.

Table 1.7

Economic crime in Luxembourg

X_j	Features	Data	Normalized data
X_1	Experience of economic crime	42%	0,37
X_2	Low confidence in law enforcement	46%	0,56
X_3	Experience of cybercrime	24%	0,10
X_4	Formal business ethics & compliance programme	84%	0,13
X_5	The ICT security policy	24%	0,56
Sum		x	1,70

Source: own estimations based on Global Economic Crime Survey 2016 and Eurostat data.

The percentage of companies who have a formal business ethics and compliance programme ensure the UK the first place among allanalyzed countries. However, it does not have an impact on decrease of number of crimes. More than a half (55%) of organizationshave experienced economic crime, which is much more than the global average. Nearly one third of reported frauds were committed by the staff (with many

more involving some degree of collusion). What is more, the percentage of frauds committed by older senior employees has been rising significantly since 2014.[15]

Table 1.8

Economic crime in UK

X_j	Features	Data	Normalized data
X_1	Experience of economic crime	55%	0,68
X_2	Low confidence in law enforcement	49%	0,67
X_3	Experience of cybercrime	44%	0,59
X_4	Formal business ethics & compliance programme	86%	0,00
X_5	The ICT security policy	32%	0,26
Sum		x	2,19

Source: own estimations based on Global Economic Crime Survey 2016 and Eurostat data.

So for most of companies, it is a question of when, not if, they will experience such offence.It is not enough to have a compliance programme, it must be well-designed to offer a clear strategic benefit to the business. Even the most rigorous compliance programme will fail, if a company's culture allows or accepts wrong-doing as an acceptable way of doing business. Companies should focus on identifying potential frauds more quickly and efficiently.Usually, at the begging of any economic crimethere isa poor decision driven by a human behavior. For this reason,employees should be the first area where the solution is looked for.

Cyprus is a country that should be set as an examplehow to deal with economic crime. Only 27%of respondent companies have experienced that kind of offence there. It means that detectingand preventing economic crime is a good recipe. Lack of confidence in local law enforcement in Cyprus is lower than in other countries. Economic crime is ever-evolving, continuously becoming a more complex issue for organisations and economies as awhole. The regulatory landscape, too, is changing, bringingwith it numerous challenges for doing business. With local lawenforcement perceived to be able to make a visibledifference, the responsibility lies not only on the companies. The burden of preventing, protecting andresponding to economic crime rests not only on organisationsthemselves.It can be said that economic crime is

[15] http://www.pwc.co.uk/forensic-services/assets/gecs/gecs-uk-brochure-2016.pdf

receiving more attention in Cyprus thanin other countries. Interestingly, low level of formal business ethics and compliance programmedoes not adversely affectthe level of crime.

Table 1.9

Economic crime in Cyprus

X_j	Features	Data	Normalized data
X_1	Experience of economic crime	27%	0,00
X_2	Law confidence in law enforcement	31%	0,00
X_3	Experience of cybercrime	20%	0,00
X_4	Formal business ethics & compliance programme	70%	1,00
X_5	The ICT security policy	37%	0,07
Sum		x	1,07

Source: own estimations based on Global Economic Crime Survey 2016 and Eurostat data.

It should be noted that economic crime in Poland is still a serious problem, but in comparison with other countries the situation is not so bad. In the last 24 months 36% of Polish companies have experienced that kind of offence which is equal to the global average. In Poland, the biggest problem is a lack of confidence in law enforcement. Much more than a half (58%) of surveyed organizations believe that law enforcement does not have adequateresources to investigate economic crime. Clearly, it is importantfor companies to have a proper investigative protocol inplace to make sure that any alleged fraud is internally investigated before turning the findings over to the law enforcement. But it must be said that Polish companies inefficiently use the potential of ethical organizational culture.

Regarding to the results of the study, ethics or compliance programme normally works in 80% of the enterprises, but only less thanhalf of them are carried out regular training in ethics.The percentage of companies which have the ICT security policy addressed the risks of destruction or corruption of data due to an attack or by unexpected incident is also the lowest in a comparison with other analysed countries.Hence, it can be stated thatthese are the main areas for improvement.

Almost one thirdof Swedish respondents of Global Economic Crime Survey have been victims of economic crime in the last two years. What is more

important,more organizations, according to the latest survey have carried out risk assessments of this kind of offence.It means that the establishment of risk-based control and work with ethical guidelines reducethe risk of being hit.Nevertheless, the indispensable condition is to build a proper, effective compliance programme. More companies are prepared for financial frauds, greater are the possibilities to minimize their impacts.

Swedish companies have the best results in having the information and communication technologies security policy addressed the risks of destruction or corruption of data due to an attack or by unexpected incident. It means that the enterprises are aware of the importance of its ICT systems and the relevant potential risks.

Table 1.10

Economic crime in Poland

X_j	Features	Data	Normalized data
X_1	Experience of economic crime	36%	0,22
X_2	Law confidence in law enforcement	58%	1,00
X_3	Experience of cybercrime	32%	0,29
X_4	Formal business ethics & compliance programme	80%	0,38
X_5	The ICT security policy	12%	1,00
Sum		x	2,89

Source: own estimations based on Global Economic Crime Survey 2016 and Eurostat data.

Moreover, the existence of this kindof security policy implies an enterprise's strategy to safeguard data and ICT systems as well as mandatory obligations for all employees.In order to prepare this tooleffectively, a formally defined policy should refer to an assessment of ICT security risks in terms of likelihood of occurrence of incidents and their possible impact on the operations of the enterprise. In addition, the policy should describe the various actors and their responsibilities in relation to incident handling and possible contingency plans.[16]Swedish may serve as an example of the proper use of the tools of defence against economic crime.

[16] http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises

Table 1.11

Economic crime in Sweden

X_j	Features	Data	Normalized data
X_1	Experience of economic crime	27%	0,00
X_2	Law confidence in law enforcement	52%	0,78
X_3	Experience of cybercrime	48%	0,68
X_4	Formal business ethics & compliance programme	81%	0,31
X_5	The ICT security policy	39%	0,00
Sum		x	1,77

Source: own estimations based on Global Economic Crime Survey 2016 and Eurostat data.

Discussion. The aggregate results of individual countries show that Cyprus copes with economic crime most effectively. The most probable cause of this success is the high confidence among companies that law enforcement can handle any threats of a fraud. It is important that enterprises believe in ability of authorities to investigate this kind of offence. Business community must feel that law enforcement understands and keep pace with all crime risks that all companies encounter.

Companies from the second place country - Luxembourg, have a low experience with cybercrime. Nowadays,this is the key to success,because this kind of offence is the second most common economic crime and there is a high probability that in the future it will become the first.This means that companies need to specialize in detecting this type of events and learn how to respond to them quickly. This is a vital challenge because of the rapidly changing technological progress, which makes this type of crime particularly difficult to detect.

The worst situation is in France, where companies are increasinglybecoming victims of fraud: 68% this year is up 13 points from the PwC study published in 2014. This rate is significantly above global average (36%). As the number of enterprises fraud victims has remained stable in the world since 2011,it has almost doubled over the same period in France. Above all, this increase should be explained

by the explosion of cybercrime.More than half of French companies do not have yet any operational action plan to respond to a cyberattack.[17]

Table 1.12

Summary data for the analysed countries

Countries	Data
Cyprus	1,07
Luxembourg	1,70
Sweden	1,77
United Kingdom	2,19
Belgium	2,28
Poland	2,89
Netherlands	3,14
France	3,42

Source: own estimations based on Global Economic Crime Survey 2016 and Eurostat data.

On the one hand, there should be noted lack of preparation by companies, and on the other hand the lack of preparation of countries and their legal system. In France and Poland companies do not trust the authorities. They are not convinced that they have sufficient tools to fight with economic crime. Respondents from all over the world gave the viewon whether theybelieve local law enforcement to be adequately resourcedand trained to investigate and prosecute economic crime.A resounding majority – 44% to 28% – expressed doubts onthis point, while a further 28% could not answer.[18]This could be a result of several divergent factors.Primarily, the opinion of the authorities may be affected by the level of economic crime itself. This means that some respondents may have a grudge against the governmenteven though they should primarily blame themselves. It is still possible thatauthorities downplaythe problem and there is a large lack of knowledge about this kind of crimes.

[17]PwC, Global Economic Crime Survey 2016, http://www.pwc.fr/assets/files/pdf/2016/03/pwc_infographie1_global_economic_crime_survey.pdf.
[18]PwC, Global Economic Crime Survey 2016, http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf, p. 13.

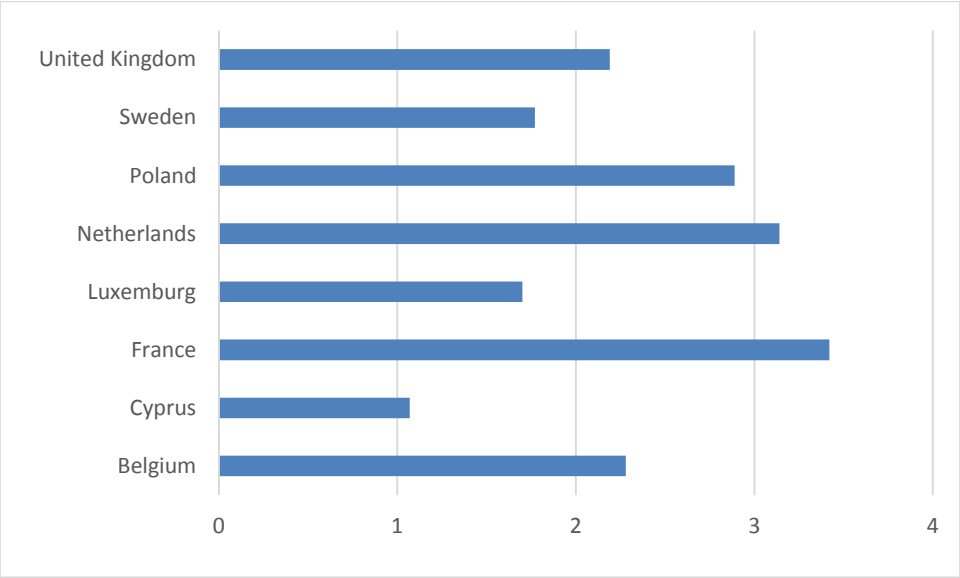


Figure 1.11. Levels of economic crime in 2016 for the analysed countries

Source: own estimations based on Global Economic Crime Survey 2016 and Eurostat data.

In order to explain which factors have the strongest relationship with level of economic crime for selected countries (estimated as synthetic variables q_i), the Pearson correlation analysis was conducted. Below in the table, we present the results of this examination.

Table 1.13

Summary data for the analysed countries

X_j	Features	Pearson correlation coefficient	The strength of relationship
X_1	Experience of economic crime	0,6856	Strong
X_2	Low confidence in law enforcement	0,6825	Strong
X_3	Experience of cybercrime	0,6335	Strong
X_4	Formal business ethics & compliance programme	0,1682	Very weak
X_5	The ICT security policy	-0,6634	Strong

Source: own estimations based on Global Economic Crime Survey 2016 and Eurostat data.

All three features which has been chosen as stimulants (experience of economic crime, low confidence in law enforcement and experience of cybercrime)are strongly positively related with economic crime level. The ICT security policy is strongly

negatively correlated with the level of economic crime, which means that this feature has a strong decreasing effect on this phenomenon.

However, one of destimulants –the percentage of companies which have a formal business ethics and compliance programme, does not correlate negatively as it should. Nevertheless, the strength of relationship is very weak, which means that this feature does not have an impact on decreasing economic crime level in selected European countries.This confirms the hypothesis stated in this article that having formal business ethics and compliance policy does not ensure sufficient protection against economic crime.

In conclusion, it is clear that success in fight against economic crime is not associated with formal business ethics and compliance programme. It is possible that such programmes are not keeping up with changing business risks. Moreover, this programme must be associated withICT security policyand both tools must interact with each other.

It should be also highlighted that economic crime is associated with generating high losses, which are difficult to estimate, especially considering the fact that actual financialloss is often only a small component of the fallout from a seriousincident.We must therefore do everything to increase their detection. It is the responsibility of the authorities, but also the companies themselves.

Works cited list:

1. Brody R.G., Mulig E., Kimball V., *Phishing, pharming and identity theft*, Academy of Accounting and Financial Studies Journal 11 (3), 43, 2007.
2. Kukuła K., Bogocz D., *Zero Unitarization Method And Its Application In Ranking Research In Agriculture*, Economic and Regional Studies, Volume 7, No. 3, 2014
3. Kukuła K., *Propozycja budowy rankingu obiektów z wykorzystaniem cech ilościowych oraz jakościowych*, QuantitativeMethods In Economics, Vol. XIII, No. 1, Warsaw 2012
4. PwC Polska, *Badanie Przestępczości Gospodarczej w Polsce 2016 - Wyniki i kluczowe wnioski*, Warsaw, March 2016, www.pwc.pl/pl/pdf/badanie-przestepczosci-gospodarczej-w-polsce-2016.pdf, (access: 30.03.2016).
5. PwC, Global Economic Crime Survey 2016, *ResultatfrånSverige*, www.cdn2.hubspot.net/hubfs/315629/Crime_Survey/crime-survey_2016.pdf?t=1459431061557, (access: 30.03.2016).
6. PwC, Global Economic Crime Survey 2016, *Belgium report*, www.pwc.be/en/documents/media-centre/publications/2016/gecs-2016-report-pwc-belgium.pdf, (access: 28.03.2016).

7. PwC, Global Economic Crime Survey 2016, *Country summary: Key findings in Cyprus*, www.pwc.com.cy/en/publications/assets/global-economic-crime-survey-2016-cyprus-findings.pdf, (access: 29.03.2016).
8. PwC, Global Economic Crime Survey 2016, *La fraudeexploseen France la cybercriminalité au cœur de toutes les préoccupations*, www.pwc.fr//assets/files/pdf/2016/03/pwc_ad_fraude_mars2016_v3.pdf, (access: 30.03.2016).
9. PwC, Global Economic Crime Survey 2016, *UK report – Old Dogs, New Tricks*, www.pwc.co.uk/forensic-services/assets/gecs/gecs-uk-brochure-2016.pdf, (access: 28.03.2016).
10. PwC, Global Economic Crime Survey 2016, www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf, (access: 25.03.2016).
11. Sobczyk M., *Statystyka – aspekty praktyczne i teoretyczne*, UMCS, Lublin 2006.
12. Whittaker, C., Ryner, B., Nazif, M., *Large-Scale Automatic Classification of Phishing Pages*, NDSS (Vol. 10), 2010, February.
13. www.ec.europa.eu/eurostat, (access: 30.03.2016)
14. www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html, (access: 30.03.2016).
15. www.pwc.fr/assets/files/pdf/2016/03/pwc_infographie1_global_economic_crime_survey.pdf(access: 30.03.2016).

1.5. КОНКУРЕНТНА РОЗВІДКА ТА КОНТРРОЗВІДУВАЛЬНА ДІЯЛЬНІСТЬ ЯК ФУНКЦІЇ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

КОЗАЧЕНКО ГАННА ВОЛОДИМИРІВНА*, д.е.н., профессор*
Полтавський національний технічний
університет імені Юрія Кондратюка
ЖИВКО ЗІНАЇДА БОГДАНІВНА, д.е.н., *профессор,*
Львівський державний університет внутрішніх справ

На сучасному етапі розвитку суспільства, коли посилюється боротьба за природні ресурси, зростає рівень конкуренції, а ситуація на світовому фінансовому ринку є складно прогнозованою, розвідувальна та контррозвідувальна діяльність є одним з найсуттєвіших засобів конкурентної боротьби. Ця теза стосується як макрорівня, де державна розвідка в сфері економіки реалізується через глибоке проникнення в інформаційне поле країн-конкурентів, і, як правило, здійснюється законними і забороненими законом методами й прийомами, спрямована на отримання необхідної інформації для коригування державної політики, в тому числі для підтримки свого національного товаровиробника та забезпечення необхідного рівня національної безпеки, так і мікрорівня стосовно кожного окремого економічного агента.

Для підприємницьких структур забезпечення конкурентної позиції та протистояння негативним впливам зовнішнього середовища неможливе без отримання інформації про дії конкурентів, зміну попиту на продукцію чи послуги, перспективні наукові дослідження та новітні технології. Виникають два протиріччя, дві тісно взаємопов'язані обставини: підприємець вимушений виступати як захисник своїх таємниць (цінної комерційної інформації); підприємець повинен з метою посилення своєї конкурентної позиції здобувати (красти, купувати) чужі таємниці, що перебувають під захистом.

Отже, забезпечення економічної безпеки можливе за умови максимально можливого втаємничення конкурентно значимої інформації, що стосується

власного бізнесу, та якомога повнішої інформаційної відкритості конкурентів, щоб своєчасно розпізнати їхні наміри й плани. Звідси випливає актуальність дослідження розвідувальної та контррозвідувальної діяльності в контексті функціонування системи економічної безпеки підприємства.

Концепцію конкурентної розвідки сформульовано наприкінці XX століття відомим американським економістом, професором Гарвардської бізнес-школи М. Портером, який визначив розвідку як інструмент досягнення конкурентних переваг і обґрунтував необхідність її застосування в цивілізованому ринковому середовищі [9, с. 489]. Проте використання розвідки в бізнесі розпочалося набагато раніше, а її трактування та завдання з часом змінювалися [7].

На відміну від розвинутих країн світу в Україні робляться лише перші кроки на шляху теоретичного обґрунтування ролі та завдань розвідувальної діяльності, зокрема і через переклад іноземних наукових джерел [1,2,3,4,5,6,8]. У результаті у вітчизняній літературі зустрічаються різноманітні поняття щодо розвідки у сфері економіки, а саме: економічна розвідка, економічне шпигунство, конкурентна розвідка, бізнес-розвідка, ділова розвідка, комерційна розвідка, промислове шпигунство, бізнес-шпигунство. Усі вони у найбільш загальному вигляді передбачають активні дії, скеровані на збір, зберігання, накопичення і обробку цінної інформації, закритої для доступу сторонніх осіб. Але поняття щодо розвідки у сфері економіки розглядаються переважно як вид діяльності, а не у контексті функціонування системи економічної безпеки підприємства.

Забезпечення економічної безпеки підприємства є призначенням найважливішої підсистеми управління – системи економічної безпеки. За найпоширенішим поглядом система економічної безпеки підприємства розглядається як сукупність взаємопов'язаних заходів організаційно-економічного та правового характеру, що здійснюються з метою захисту діяльності підприємства від реальних чи потенційних негативних впливів внутрішнього та зовнішнього середовища й уможливлюють його розвиток.

Функціонування системи економічної безпеки підприємства відбувається завдяки виконанню її функцій. Незважаючи на наявність значної кількості наукових праць, функції системи економічної безпеки підприємства дотепер залишаються недостатньо вивченими. Серед них важлива роль належить таким функціям як конкурентна розвідка, контррозвідувальна діяльність та протидія рейдерству, реалізація яких спеціальними підрозділами служби економічної безпеки шляхом виконання сукупності завдань, описаних розробленими алгоритмами, дозволить запобігти втратам у діяльності підприємства завдяки отриманню або збереженню інформації певного призначення та ухвалення з її використанням управлінських рішень щодо його діяльності та економічної безпеки.

Розвідувальна діяльність є закономірним явищем підприємництва, важливим компонентом забезпечення економічної безпеки сучасних підприємств. Спонуканням до розвідувальної діяльності є конкуренція – найголовніший чинник, що забезпечує рівновагу системи ринкової економіки. У найзагальнішому вигляді розвідувальна діяльність передбачає активні дії, скеровані на збір, зберігання, накопичення та обробляння інформації, закритої для стороннього доступу.

У розвідувальній діяльності, пов’язаної із забезпеченням економічної безпеки підприємства, виділяють конкурентну розвідку та промислове шпигунство, які поєднує загальна мета – одержання інформації, яка б дала змогу здобути конкурентну перевагу на ринку. Головною відмінністю між ними є методи й способи отримання інформації. Конкурентна розвідка здійснюється виключно законними методами з використанням лише відкритих джерел, а промислове шпигунство передбачає нелегальні методи й технології.

Поняття "конкурентна розвідка" тлумачиться по-різному: як інструмент маркетингової діяльності, як організований процес, реалізація якого спрямована на ухвалення тактичних і стратегічних рішень, як певна організаційна структура, вид діяльності чи сукупність ресурсів, спрямованих на вирішення конкретних завдань у межах підприємства. Узагальнення цих підходів

дозволило визнати конкурентну розвідку функцією системи економічної безпеки підприємства, реалізація якої дозволяє отримати інформацію про стан та динаміку конкурентного середовища (рис. 1.12).

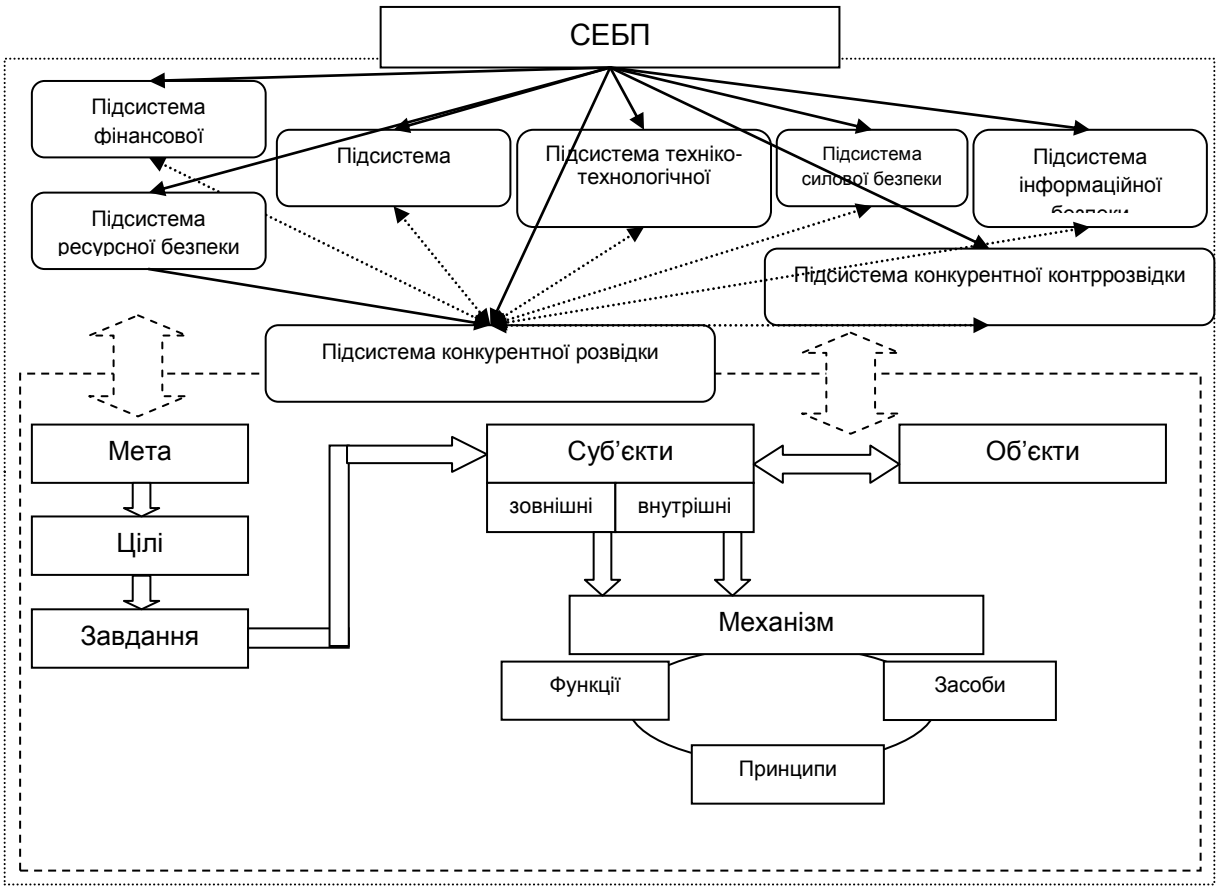


Рис. 1.12. Підсистема конкурентної розвідки у системі економічної безпеки підприємства

Головним призначенням конкурентної розвідки є випередження, недопущення виникнення нестандартних ситуацій, деструктивних подій у діяльності підприємства, які створюють економічно небезпечну ситуацію, за допомогою своєчасного отримання повної та достовірної інформації про його оточення.

Вирішувані завдання та особливості ведення конкурентної розвідки різняться за етапами життєвого циклу підприємства, адже на кожному з них його діяльності властиві особливості, які визначають не лише її характер та цілі, вектор розвитку, ринкову позицію та тип організації, а й сукупність завдань. Пріоритетні завдання конкурентної розвідки доцільно розподілити за

етапами життєвого циклу підприємства, а різновидами конкурентної розвідки визнати стратегічну, тактичну та оперативну.

Ефективність отримання розвідувальної інформації багато в чому залежить від методів збору інформації, які для цього застосовуються (за однією класифікацією – загальні, особливі та окремі, за іншою – легальні, напівлегальні й нелегальні). Використання кожного з методів доречне за певних умов.

Сталої та загальновизнаної методики конкурентної розвідки дотепер не розроблено. За результатами аналізу переваг та обмежень відомих методик конкурентної розвідки (методика Харківського об’єднання аналітиків і професіоналів конкурентної розвідки SCIP.ORG.UA; методика, що використовується членами Європейського об’єднання професіоналів конкурентної розвідки; "Методика 4С"; методика компанії AWARE; методика конкурентної розвідки 4К+1) розроблено типовий алгоритм конкурентної розвідки (рис. 1.13). Побудований алгоритм конкурентної розвідки передбачає послідовне виконання типових етапів, реалізація яких покликана доповнити результати моніторингу економічної безпеки щодо інформаційного забезпечення управління системою економічної безпеки підприємства. Наведені етапи є типовими, стандартними для сучасної служби економічної безпеки підприємства.

Поряд з отриманням достовірної інформації про конкурентне середовище підприємства не менш важливою є проблема захисту його комерційних таємниць, конфіденційної інформації, яка розв’язується за допомогою контррозвідувальної діяльності. Контррозвідка одержала легітимність і стала складовим елементом ділового процесу на підприємствах України лише з переходом підприємств до ринкових відносин економічна (промислова). Багато вітчизняних підприємств ще в 90-і рр. минулого століття на етапі становлення роботи своїх служб економічної безпеки брали приклад із західних фахівців з конкурентної розвідки, а також охоче залучали до роботи колишніх працівників спецслужб.

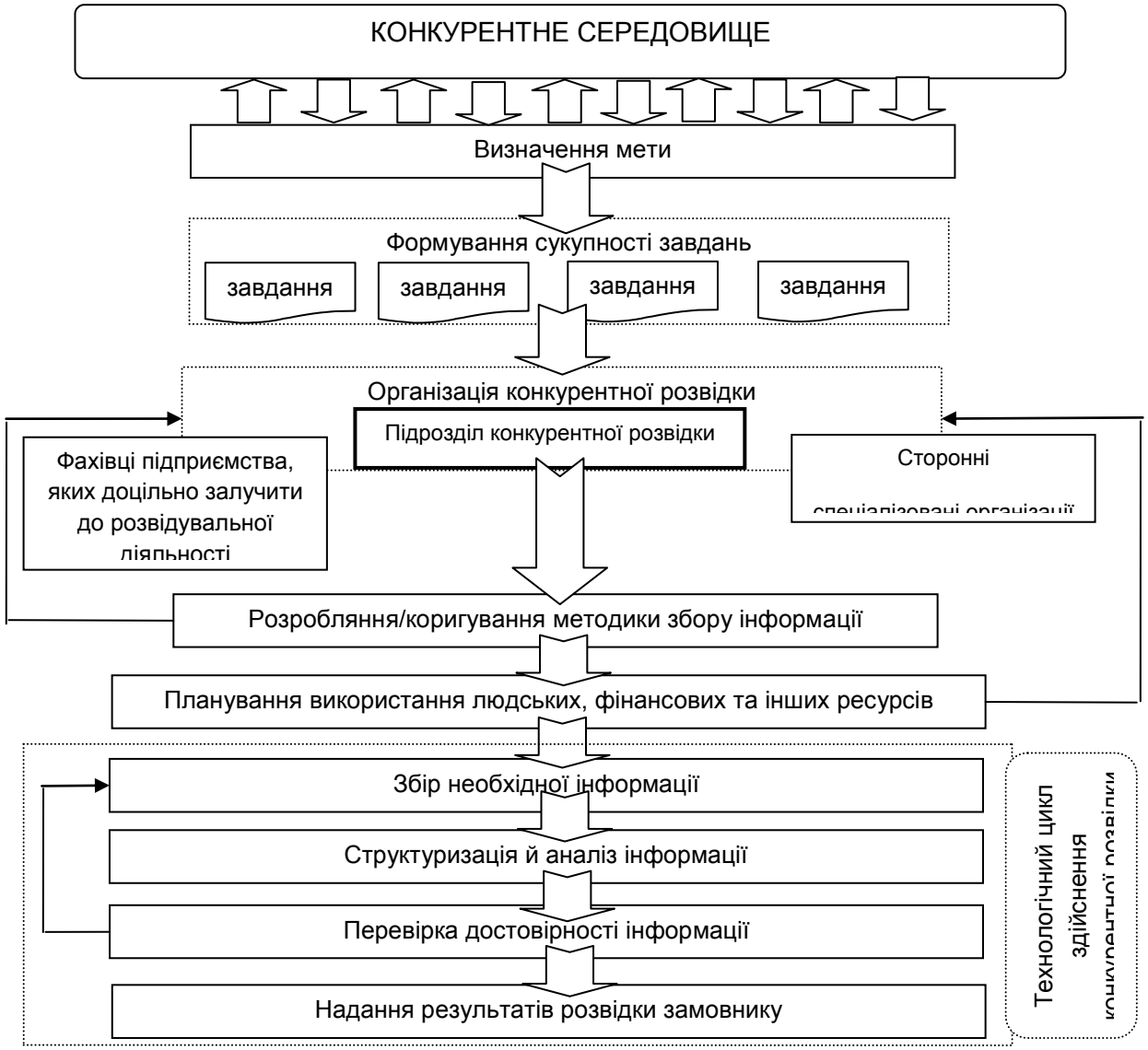


Рис. 1.13. Типовий алгоритм конкурентної розвідки підприємства

Значення і роль контррозвідки в сучасних умовах ведення бізнесу зумовлено, по-перше, прагненням деяких підприємств усунути або нейтралізувати своїх конкурентів, користуючись засобами промислового шпигунства; по-друге, криміногенною ситуацією в країні, що створює поживне підґрунтя для певних верств населення вирішувати свої проблеми злочинним шляхом; по-третє, потребою здійснення захисних дій щодо представників державних органів управління, які використовують своє службове становище у злочинних цілях.

Контррозвідувальна діяльність як функція системи економічної безпеки підприємства дозволяє запобігти втратам у його діяльності шляхом збереження комерційної таємниці та конфіденційної інформації.

Метою контррозвідки є недопущення витоку інформації про діяльність, плани та наміри підприємства. За результатами аналізу виділено три групи типових способів злочинних зазіхань на інформацію: незаконне збирання інформації, що є комерційною або банківською таємницею; незаконне використання такої інформації; умисне розголошення такої інформації.

У найзагальнішому вигляді контррозвідка в системі економічної безпеки підприємства передбачає внутрішній моніторинг (дозволяє виявити сукупність слабких місць, завчасна ліквідація яких унеможливлює реалізацію значної кількості загроз, а також дотримання працівниками підприємства внутрішніх правил з нерозголошення конфіденційних даних) та аналітичну роботу (передбачає проведення порівняльної характеристики, виявлення сильних і слабких сторін, розробляння конкретних рекомендацій для менеджменту з метою недопущення збитків, втрати частки ринку тощо).

В цілому процес конкурентної розвідки і контррозвідки в системі економічної безпеки підприємства складається з трьох взаємопов’язаних складових: внутрішнього моніторингу, зовнішнього моніторингу та аналітичної роботи (рис. 1.14).

Внутрішній моніторинг припускає, що працівники служби безпеки всіляко захищають підприємство від проникнення "шпигунів" та "розвідників", а також відстежують дотримання співробітниками підприємства внутрішніх правил з нерозголошення конфіденційних даних. Для цих потреб активно застосовуються спеціальні інформаційні системи. Зовнішній моніторинг, і є, власне конкурентною розвідкою у найзагальнішому розумінні. Він передбачає збір повного обсягу інформації про конкурентів (технології, управління, обсяги збуту, чинники конкурентної переваги, стратегічні плани на майбутнє, стратегії завоювання ринку, можливі загрози для свого підприємства, методи оптимізації роботи, інновації та ін.). Аналітична робота передбачає проведення

порівняльної характеристики, виявлення своїх сильних і слабких сторін, розробку конкретних рекомендацій для менеджменту з метою недопущення збитків, втрати частки ринку тощо.

Рис. 1.14. Конкурентна розвідка та контррозвідка як функції системи економічної безпеки підприємства

Для реалізації зазначених функцій системи економічної безпеки підприємства доцільно виділити підрозділи конкурентної розвідки та контррозвідки (рис. 1.15), визначити об’єкти їхньої діяльності, коло завдань, відповідні критерії та показники для об'єктивного оцінювання діяльності, а також проаналізувати методи, що найчистіше використовують співробітники цих підрозділів. Отже, конкурентна розвідка як вид розвідувальної діяльності підприємства є функцією системи економічної безпеки. Її здійснення уможливлює отримання інформації про стан конкурентного середовища та його зміни, що є основою для ухвалення стратегічних, тактичних та оперативних рішень у діяльності підприємства.

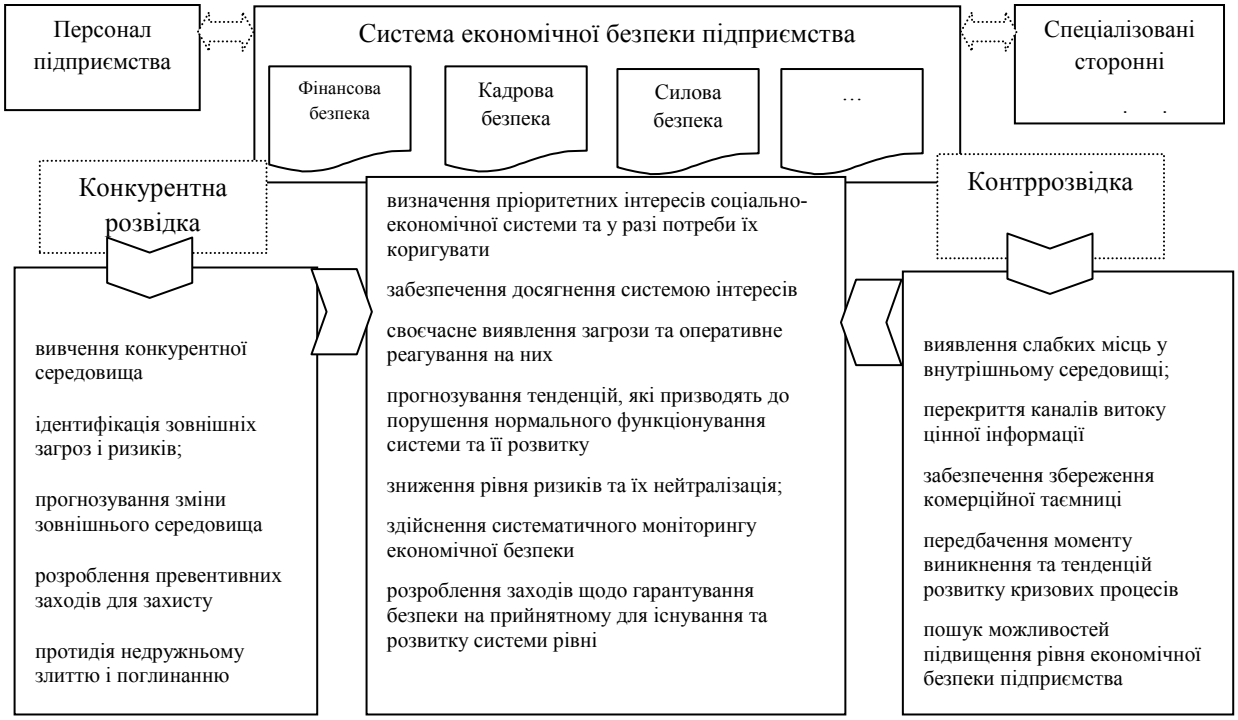


Рис. 1.15. Функції конкурентної розвідки та контррозвідки у системі економічної безпеки підприємства

Головним призначенням конкурентної розвідки є випередження, недопущення виникнення нестандартних ситуацій, деструктивних подій у діяльності підприємства за допомогою своєчасного отримання повної, достовірної інформації про його оточення. Цілі та особливості конкурентної розвідки різняться за етапами життєвого циклу підприємства, що зумовило формування її пріоритетних завдань за цими етапами.

Контррозвідувальна діяльність як функція системи економічної безпеки підприємства дозволяє запобігти втратам в діяльності підприємства, зберегти його комерційну таємницю та конфіденційну інформацію і зрештою зміцнити економічну безпеку підприємства. Але для цього контррозвідувальна діяльність має бути належним чином організована, нею не можна у наш час нехтувати.

Список використаних джерел:

1. Абрамов В. Деловая разведка в системе обеспечения предприятия / В. Абрамов // БДИ. — 2002. — № 2. — С. 22─26.

2. Бараннік Р. В. Конкурентна розвідка: уявність та реальність / Р. В. Бараннік // Право України. — 2007. — № 11. — С. 72–76.

3. Берсенёв В. Л. Феномен конкурентной разведки: основы теоретического анализа: препринт. / В. Л. Берсенёв, Е. Л. Ющук. — Екатеринбург: Институт экономики УрО РАН, 2009. — 76 с.

4. Боган К. Бизнес-разведка. Внедрение передовых технологий: пер. с англ. / Кристофер Боган, Майкл Инглиш; под общей ред. Б.Л. Резниченко. — М.: Вершина, 2006. — 314 с.

5. Борисов Н. И. Конкурентная разведка как инструмент конкурентной борьбы [Электронный ресурс] / Н. И. Борисов. — Режим доступа : http://www.marketing.spb.ru/lib-research/competition_spy.htm

6. Вайс А. Краткое руководство по конкурентной разведке: как собирать и использовать информацию о конкурентах : Часть 2 [Электронный ресурс] / А. Вайс. — Режим доступа : http://it2b.ru/blog/arhiv/767.html

7. Живко З. Б. Конкурентна (ділова) розвідка в системі економічної безпеки : [монографія] / З. Б. Живко. — Львів: Апріорі, 2008. — 192 с.

8. Івченко О. Промислове (економічне) шпигунство: конкурентна розвідка й контррозвідка [Електронний ресурс] / О. Івченко. — Режим доступу : //www.justinian.com.ua/article.php?id=707

9. Портер М. Э. Конкуренция / Майкл. Э. Портер / [пер. с англ.]. — М.: ИД "Вильямс", 2005. — 608 с.

1.6. БАНКІВСЬКІ КРИЗИ, ЯК ПЕРЕДУМОВА ВИНИКНЕННЯ ЕКОНОМІЧНИХ ЗЛОЧИНІВ У БАНКІВСЬКІЙ СФЕРІ

МІГУС ІРИНА ПЕТРІВНА, *д.е.н., професор,*
завідувач кафедри менеджменту та економічної безпеки
Черкаського національного університету імені Богдана Хмельницького
КОВАЛЬ ЯНА СЕРГІЇВНА, *магістрант*
Черкаський інститут банківської справи

Загальне соціально-економічне і політичне становище призвело до нестійкості фінансового ринку, що породило процес банкрутства банків. Ситуація ускладнюється тим, що зростаюча неспроможність банків здійснювати платежі, надавати довгострокові кредити для розвитку реального капіталу, негативно позначилась на платоспроможності підприємств і спровокувала подальший спад виробництва. Посилюються зазначені негативні тенденції впливом світової фінансовоїта внутрішньої економічної кризи, коли в умовах економічного спаду ризиковість діяльності банків суттєво підвищується, банківська система функціонує відособлено відвиробничої та торговельної сфер і, таким чином, не виконує належного, з точки зору суспільного поділу праці, функціонального призначення і навантаження.

Міжнародний досвід переконливо свідчить, що економічне зростання і забезпечення ефективних умов для розвитку приватного сектору, поліпшення соціального захисту та добробуту населення можливі лише за умов сталого розвитку банківської системи як одного з головних елементів ринкової економіки. Одним з напрямків забезпечення фінансової стійкості та розвитку банківської системи України є розробка теоретичного базису реалізації антикризового управління в процесах функціонування та розвитку вітчизняних банків [2].

Банківська діяльність завжди супроводжується ризиками, а гонитва за над прибутками значно посилює це явище і, разом з іншими чинниками, ускладнює процес забезпечення фінансової стабільності банків, про що свідчить сучасний, майже кризовий стан вітчизняної банківської системи.

Крім того, банківська діяльність завжди супроводжується ризиками, а гонитва за над прибутками значно посилює це явище і, разом з іншими чинниками, ускладнює процес забезпечення фінансової стабільності банків, про що свідчить сучасний, майже кризовий стан вітчизняної банківської системи.

Кожен банк реалізує стратегічні завдання своїх акціонерів шляхом розробки відповідної політики та програм залучення клієнтів: банк відображає у системі відносин між постачальниками та споживачами банківських послуг певні специфічні цільові установки акціонерів, які об'єктивно сформувалися у суспільстві, суб'єктивно визначилися в цільових завданнях власників і відтворилися у стратегічних програмах розвитку банків [15].

Актуальність реалізації антикризового управління в діяльності банків обумовлена нестабільністю політичної та економічної ситуації в країні, що породжує значну кількість ризиків, які банки змушені приймати в процесі здійснення банківських операцій та надання послуг. У зв'язку з цим зростає важливість розроблення й обґрунтування таких механізмів управління в банківському секторі, які б дали змогу мінімізувати можливість виникнення фінансових криз і забезпечити фінансову стійкість банківського сектору.

У виникненні та розвитку кризових явищ помітно зросла роль банків, оскільки саме вони формують інституційну систему, впливаючи на ефективність розподілу кредиту, структуру процентних ставок, рішення у сфері грошово-кредитної політики та їх ретрансляцію економічним агентам. Це пояснюється тим, що стратегія поведінки окремих банків формується у результаті прийняття рішень на мікрорівні, хоча після колективних дій вони впливають на формування макроекономічних умов, у яких існують як самі банки, так і інші економічні агенти. Подібна роль банківського сектора економіки зумовлюється його стало випереджаючою реакцією на зміни у кон'юнктурі порівняно з іншими її секторами, що дозволяє використовувати його поведінку як дійовий інструмент прогнозування економічної ситуації [20].

Залежно від мети та предмету свого дослідження різні науковці по-різному трактують сутність банківської кризи: одні вчені визначають банківську кризу

як руйнування зв'язків між елементами системи, інші – як закономірну форму оновлення діючої системи управління грошовими потоками і національними фінансами (табл. 1).

Таблиця 1.13

Аналіз наукового поняття «банківська криза» згідно різних наукових аспектів

Науковці	Трактування
Барановський О.І. [2]	ситуація, за якої проблеми, що виникають в банках, призводять до істотного зменшення капіталу банківської системи.
Коваленко В.В. [17]	криза банківського сектору характеризується ненормально низьким рівнем економічної діяльності банків протягом тривалого часу.
Вовк В.Я. [6]	ситуація, коли приватний та корпоративний сектори економіки потерпають від значної кількості банкрутств, а фінансові інститути і корпорації мають значні труднощі з виплатами за укладеними контрактами.
Тавасієва А.М. [31]	це стрімке та масштабне погіршення якості діяльності великої кількості банків, що проявляється у нездатності значної кількості кредитних організацій
Ковзанадзе І.К. [19]	ситуацією погіршення якості банківських активів, атакож відповідного погіршення фінансових результатів діяльності великої кількості банків, виникнення у них проблем з ліквідністю під впливом кризових чинників у контексті системної банківської кризи.
Клюско Л.А. [18]	стан банківської системи, коли вартість фінансових інструментів несподівано і різко зменшується.
Смовженко Т.С. [25]	пропонує розуміти фактичний або потенційнийстан, що виникає в процесах функціонування і розвитку банківської системи, спричиняє руйнування її економічного потенціалу та ставить під загрозу подальший розвиток.
Зарицька І.М. [12]	глибоке розбалансування банківської системи, що проявляється через неспроможність суб'єктів системи ефективно виконувати свої функції

Джерело складено автором на основі [14]

Безперечно, кожне подане визначення тим чи іншим чином розкриває зміст поняття «банківська криза» і тому заслуговує на увагу.

На основі розглянутих поглядів представимо власне бачення даного поняття. На наш погляд, кризою банківської системи варто вважати різке погіршення стану ринку банківських послуг під впливом внутрішніх і зовнішніх факторів, що призводить до не дієздатності окремих банків,

погіршення ліквідності й якості фінансових інструментів, зниження рівня надійності та стабільності функціонування банківської системи в цілому [28].

Крім того, представлені визначення дозволяють нам сформувати видову класифікацію банківських криз (табл. 1.14).

Таблиця 1.14

Видова класифікація банківських криз

Ознака	Розподіл
1. За жорсткістю і глубиною наслідків	Перший тип (на мікроекономічному рівні незалежно від величини бюджетних витрат). Другий тип (більші витрати та руйнівні наслідки, що поширюються на макроекономічний рівень). Третій тип (повномасштабна бюджетно-фінансова дестабілізація, яка призводить до високого рівня інфляції, демонетизації економіки, стрімкого падіння фінансових індикаторів та поширюється на всю економічну систему (можливий дефолт).
2. За географічним поширенням	Світова (охоплює банківські системи та національні економіки країн більшості основних регіонів світу). Регіональна (охоплює банківські системи країн певного регіону, може бути спричинена схожими причинами). Локальна (місцева) (охоплює банківську систему окремої країни, діє в межах національного масштабу, зумовлена, переважно, внутрішніми макроекономічними чинниками).
3. За ступенем ураження	Глобальна (охоплює банківські системи та національні економіки більшості основних країн). Макрорівень (охоплює банківську систему, економіку країни). Мікрорівень (розповсюджується на окрему кількість банків країни).
4. За рівнем складності	Проста (характеризується негараздами лише в банківській системі). Подвійна (банківська криза + валютна криза або криза заборгованості). Потрійна (банківська криза + валютна криза + криза заборгованості).
5. За формою прояву	Явна (передує банківська паніка, припинення видачі депозитів вкладникам, банкрутство банків). Прихована (неспроможність банків виконувати більшість своїх функцій).
6. За причиною виникнення	Кредитний тип (порушення функціонування кредитного процесу) Фінансовий тип (проблеми із валютними зобов'язаннями, власне зобов'язаннями). Політичний тип (проявляється у протекціоністській і реформаційних формах).
7. За тривалістю	Довгострокова (значний період протікання – більше 1 року). Короткострокова (період протікання – до 1 року)
8.За періодичністю	Періодична (регулярна повторюваність через певніпроміжки часу) Проміжна (переривання на будь-якому етапі)
9. За рівнем передбачуваності	Прогнозована (закономірне, регулярнее явище). Не прогнозована (несподіване, раптове явище, форс-мажор)

Джерело складено автором на основі [13]

Таким чином, можна сказати, банківська криза – це один із видів негативного прояву глобалізаційних процесів. Залежно від мети та предмету

свого дослідження різні науковці по-різному трактують сутність банківської кризи: одні вчені визначають банківську кризу як руйнування зв'язків між елементами системи, інші – як закономірну форму оновлення діючої системи управління грошовими потоками і національними фінансами [3].

Поряд з визначенням змісту банківської кризи та її форм та різновидів вчені приділяли увагу дослідженню основних причин виникнення та протікання банківських криз в країні. Узагальнення різнопланових поглядів та підходів науковців дозволили визначити фактори, що впливають на виникнення банківської кризи (рис. 1.16).

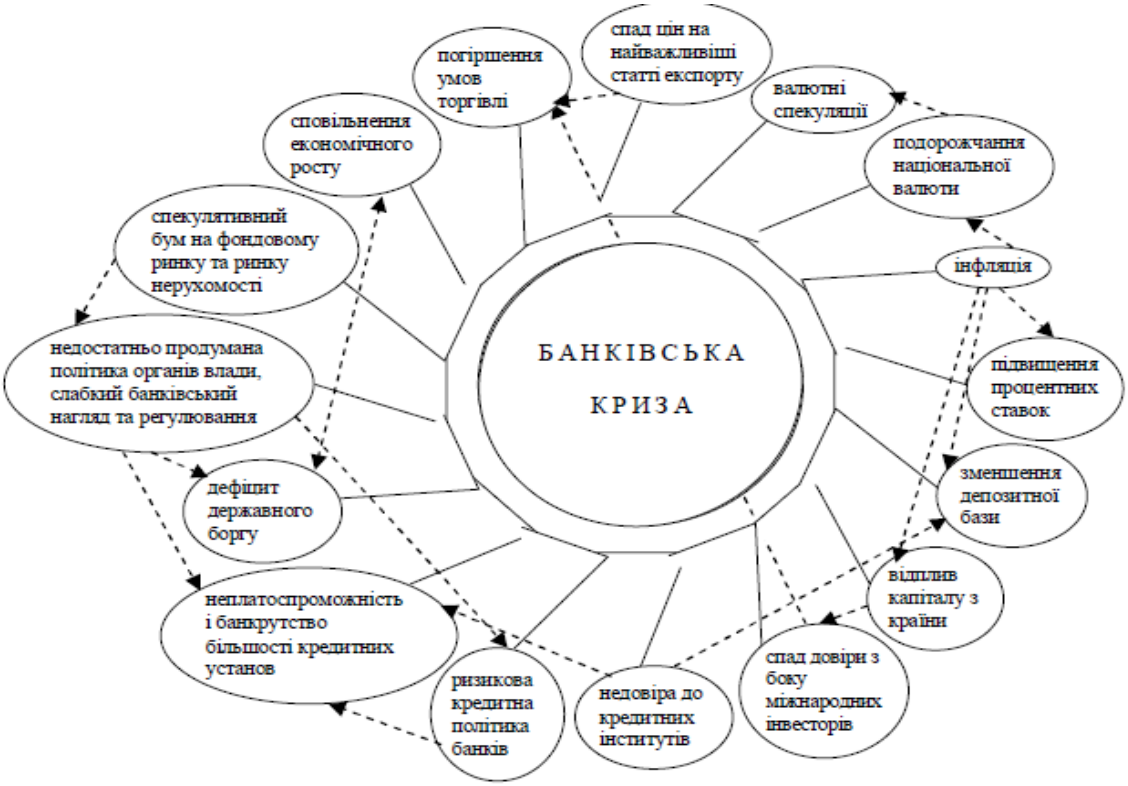


Рис. 1.16. Основні причини, що обумовлюють банківську кризу

Джерело складено автором на основі [11]

Банківська сфера, з огляду на стан розвитку, характер взаємозв'язків, проблеми та специфічні особливості функціонування, може перебувати в різних станах – таких, зокрема, як ефективна рівновага, неефективна рівновага, ефективна нерівновага, не ефективна нерівновага (рис. 1.17) [8].

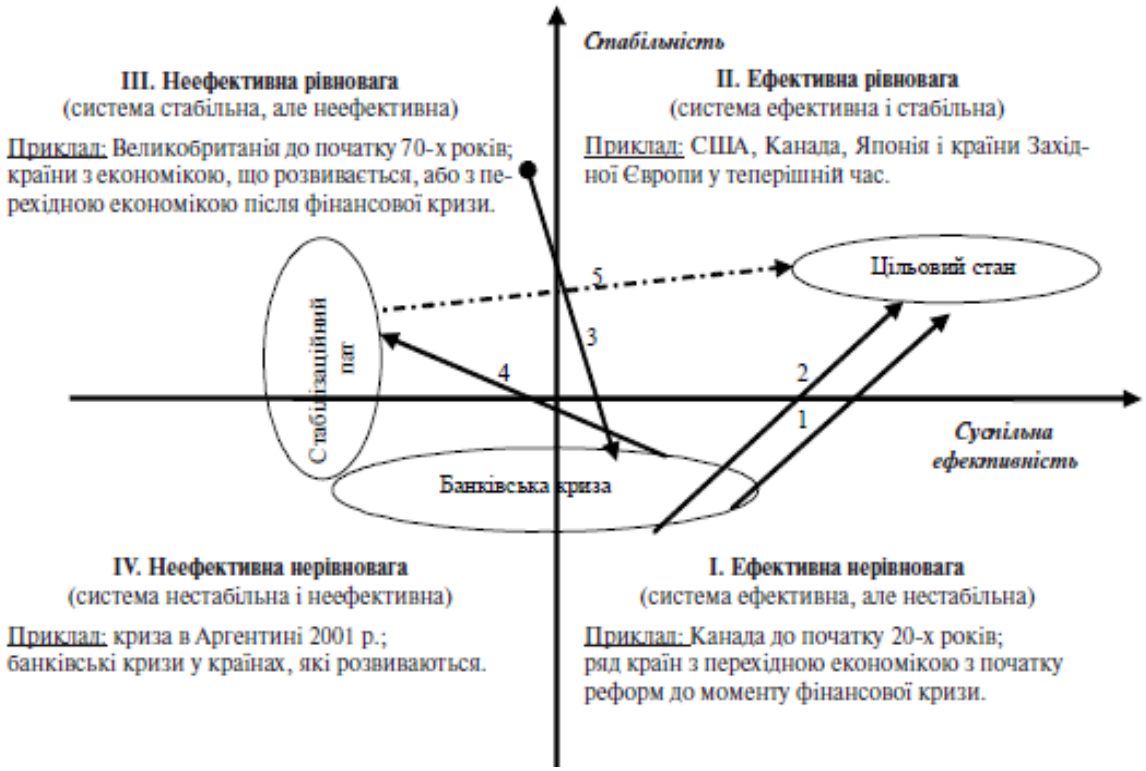


Рис. 1.17. Класифікація станів банківської системи у просторі «стабільність – ефективність»

Цифрами позначено:1,2 – «природні» еволюційні траєкторії країн Заходу у XIX – XX ст; 3 - початкова стадія формування й розвитку комерційних банківських систем у країнах з перехідною економікою; 4 – колапс банківської системи у ході кризи та її перехід у стан «стабільного пата»; 5 – бажана траєкторія посткризового розвитку банківської системи в перехідній економіці.

Джерело [22]

Фактори виникнення банківської кризи і механізми їх впливу на банківську систему наведено в таблиці 3. Кризові прояви спостерігаються практично на всіх фінансових ринках. При цьому кожна фінансова криза останніх десятиріч є своєрідною і відрізняється від попередніх. Проте часом фактори, що сприяли її розвиткові, схожі. Так, спільними факторами, що мали місце в усіх системних банківських кризах країн, які розвиваються, є лібералізація місцевої фінансової системи; концентрація спекулятивного капіталу на місцевих фінансових ринках; низька капіталізація банківської системи та її слабкість; концентрація внутрішніх позик у галузях, залежних від

зовнішніх ринків; не достатній розвиток фінансових інститутів; збільшення частки неповоротних кредитів [23].

Крім того, досить часто факторами банківських криз є прийняття банками на себе надмірних ризиків; погане управління; недостатній внутрішній контроль або його відсутність; акцент на збільшенні ринкової частки банку, а не на прибутковості; про рахунки у валютній політиці; розрив вимог і зобов'язань по строках у самих банків або у їх позичальників.

Таблиця 1.15

Фактори виникнення банківської кризи і механізми їх впливу на банківську систему

Фактори	Механізми впливу на банківську систему
Не сприятливі зміни цін на основних для країни експортних та імпортних ринках	Різке зниження цін на традиційні експортні товари або різке зростання вартості імпорту спричиняють втрату валютних доходів для країни в цілому та експортерів, що може зумовити збитки для банків, які їх обслуговують.
Переважання короткострокових зобов'язань у структурі боргу	Висока питома вага короткострокових зобов'язань, внаслідок необхідності направлення країною значних коштів на обслуговування зовнішнього боргу, накладає на банки великі обмеження у проведенні активних операцій.
Реальне подорожчання національної валюти	Переоціненість національної валюти у реальному вираженні призводить до скорочення чистого експорту і формує девальваційні очікування, які можуть спровокувати вилучення депозитів вкладниками банків.
Високі процентні витрати по внутрішньому боргу	Зростання доходності по внутрішніх зобов'язаннях означає, з одного боку, зростання процентних доходів, а з іншого – зниження ринкової вартості придбаних цінних паперів.
Висока вартість запозичень на ринку МБК	Зростання процентної ставки в умовах перевищення строковості активів банків над строковістю зобов'язань спричиняє підвищення вартості фондування.
Високий рівень фінансових ризиків у банківській системі	Недостатність наявного капіталу у відношенні до прийнятих ризиків, слабке покриття зобов'язань ліквідними активами, дисбаланс між валютними активами і зобов'язаннями, висока частка прострочених позик у кредитному портфелі банків можуть спричинити як банкрутство окремого банку, так і широкомасштабну банківську кризу.
Уповільнення економічного зростання	Зниження темпів економічного зростання спричиняє погіршення платоспроможності країни, звуження можливостей банківських позичальників щодо обслуговування боргу.
Інфляція	При проведенні курсу на придушеня інфляції банківська система опиняється під ударом.
Відкритість економіки	Як свідчить практика, фінансова лібералізація спричиняє нагромадження у банків "поганих" боргів.

Фактори	Механізми впливу на банківську систему
Валютизація активів банківської системи (в цілому або окремих статей активів)	Зміна частки активів, номінованих в іноземних валютах,свідчить про недовіру банківської системи до стабільності національної валюти, а зміна частки залучених коштів, особливо депозитів населення (з урахуванням поправки на дохідність), – про недовіру населення.

Джерело складено автором на основі [18]

Як свідчать окремі дослідження, частота банківських криз, пов'язаних з валютними, є вищою, ніж частота валютних криз, пов'язаних з банківськими.

Тому банківська система має великі можливості впливати на розвиток економіки, але водночас на ній відбиваються наслідки недосконалості економічної концепції, неврегульованість певних правових норм, недоліків кредитно-банківських технологій, документообігу, недостатнього професійного рівня працівників та зловживань з боку співробітників установи та її клієнтів. Однією з особливостей банківської системи є дуже великий обсяг коштів, які в ній акумульовані. Враховуючи це вона досить приваблива для осіб, які мають наміри протиправного збагачення. Саме тому кредитно-фінансова сфера вважається однією з найбільш криміногенних [6].

Необхідно пам'ятати, що у банківських криз немає чітких кількісних характеристик початку й завершення. Питання виміру глибини та масштабів банківської кризи, як і самого факту її початку й завершення, трактуються в економічній літературі неоднозначно. Але припинення операцій навіть одного великого банку може виявитися достатньо, щоб викликати системну кризу – ланцюгову реакцію не платоспроможності цілого ряду банків країни та зупинку всієї її платіжної системи.

На практиці межу між кризою банківської системи і проблемами окремих банків важко окреслити однозначно, оскільки проблеми їх неспроможності можуть накопичуватись і починати стосуватися дедалі більшої кількості банків, посилюючи загрозу їх одночасного банкрутства.

Зростання безнадійних активів, збиткова діяльність і втрата власного капіталу характеризують окремий банк як проблемний. Але для характеристик і ситуації у банківській системі як банківської кризи проблемними мають стати

значна кількість банків, що у рамках економічної системи виражається в їх нездатності виконувати свої основні функції – акумуляції та мобілізації тимчасово вільних коштів, надання кредитів, проведення розрахунків і платежів в економіці країни [31].

При цьому банківські кризи мають свої специфічні особливості. Так, по-перше, на відміну від циклічних економічних криз, зумовлених безпосередньо специфічними особливостями відтворення промислового капіталу, банківські кризи не мають циклічного характеру. Відображаючи продовження процесу виробництва у сфері обігу і, з огляду на це, будучи пов'язаними з відтворенням промислового капіталу, вони, на відміну від циклічних криз, великою мірою пов'язані з психологією суб'єктів фінансового ринку (довіра чи недовіра до уряду, центрального і комерційних банків). По-друге, істотне значення для виникнення й перебігу банківських криз мають недоліки в управлінні діяльністю банків і банківських холдингів з боку не тільки банківських менеджерів різних рівнів, але й державних структур, які регулюють банківську діяльність, а також центральних банків.

Кожна банківська криза, що сталася в останні роки, є своєрідною і відрізняється від попередніх. Виникнення кризи банківської системи може негативно вплинути на стійкість інших сегментів фінансового ринку, а також на показники доходності небанківських фінансових установ внаслідок значної присутності банківських фінансових інструментів у їх інвестиційних портфелях. А той факт, що частина суб'єктів фінансового сектора є дочірніми структурами банків або входять до складу банківських конгломератів, посилює схильність до системної кризи всього фінансового сектора [1].

Таким чином, істотна роль банків у виникненні та перебігу кризових явищу життєдіяльності різних держав світу і світової цивілізації в цілому зумовлює значущість ретельного дослідження теоретичних течій і підходів до визначення сутності, причин і наслідків банківських криз, а також до виявлення їх моделей і різновидів, закономірностей і особливостей прояву, взаємозв'язку і взаємозумовленості з валютними і фінансовими кризами.

Оскільки ж перебіг кризових явищ у банківській сфері України істотно залежить від ступеня реалізації наявних і потенційно можливих ризиків, то особливої уваги потребують визначення їх сутності та особливостей прояву, забезпечення належної оцінки й розробки адекватних заходів щодо їх попередження (мінімізації) [18].

Сучасна банківська криза в Україні, що є складовою загальної фінансово-економічної кризи, зумовлена негативним впливом як внутрішніх, так і зовнішніх факторів. Так, на розвиток кризових явищ у вітчизняній банківській системі, зокрема, вплинула недосконала внутрішня макроекономічна і зовнішньо -економічна політика, що супроводжується економічним спадом і високим інфляційним тиском на економіку; низька капіталізація банків; тривала не керована кредитна експансія на фоні високих кредитних ризиків, неналежного рівня управління ними і низької якості наявних активів; існування розривів між зростанням кредитів і ВВП, активами і зобов'язаннями, строками і валютами; нерівномірний розподіл активів і капіталу між банками різних груп; істотна залежність банків від зовнішніх запозичень на фоні світової кризи ліквідності; недосвідченість банківських менеджерів; банківська паніка, викликана недовірою вкладників до банківських установ, а також банків один до одного, що супроводжувалася масовим вилученням коштів з рахунків і згортанням міжбанківського кредитування; прорахунки у валютній політиці, стрімка девальвація національної валюти і зростання спекулятивних операцій банків на валютному ринку; недосконала практика стрес-тестування і внутрішнього банківського контролю.

Враховуючи те, що з поглибленням процесів глобалізації і зростанням загальної нестабільності ринків рівень ризиків банківської діяльності зростає, необхідно відповідно до особливостей повинні реалізовувати заходи, спрямовані на запобігання виникненню або повтору банківських криз [26].

Ось чому для подолання кризових явищ у банківській системі України необхідні: проведення обґрунтованої внутрішньої макроекономічної та зовнішньо -економічної політики; якнайшвидше розв'язання проблем

реструктуризації та рекапіталізації банків; ліквідація (мінімізація) існуючих розривів між активами і зобов'язаннями банківських інститутів; гарантування міжбанківських кредитів, кредитів для малого й середнього бізнесу та надання підтримки компаніям, які не можуть залучити необхідне фінансування через проблеми у банківському секторі; зниження нормативів мінімальних резервних вимог для комерційних банків; субсидування банкам процентних ставок по кредитах громадянам на придбання вітчизняних товарів; розробка й реалізація ефективної антиінфляційної та антидевальваційної політики; збільшення розміру державних гарантійна банківські вклади; введення тимчасових адміністрацій і кураторів у банківських установах; підвищення фінансової дисципліни, дієвості банківського нагляду і внутрішнього контролю в банках.

Економічні кризи сприяють збільшенню рівня злочинності в сфері банківській діяльності є те, що вона негативно вплинула на якість та рівень життя населення нашої країни. Це призвело до погіршення соціальних показників, а саме: скорочення зайнятості, зростання безробіття, зменшення реальних доходів громадян, зниження рівня заробітних плат, зростання вартості життя, загострення проблем із житлом, зростання споживчих цін, збільшення видатків на лікування, освіту, відпочинок тощо [9].

Зменшення наслідків світової фінансової кризи та перехід до стабільного зростання великою мірою залежить від ефективного регулювання діяльності банків України державними органами та обрання необхідних інструментів регулювання. Вибір ефективних методів антикризового управління має базуватися, перш за все, на розумінні самого поняття "криза".

Криза розглядається, як фактичний стан, у якому знаходиться банківський сектор, який виникає при неприбутковій роботі, неефективному управлінні активами і кредиторською заборгованістю, що приводить до відтоку коштів і неповного задоволення вимог кредиторів, нездатності банків здійснювати фінансове забезпечення своєї діяльності. Кризу розглядають як можливий потенційний стан системи з непередбачуваними наслідками, що ставить під

загрозу її подальший розвиток, як фактичний, або потенційно можливий стан функціонування банківського сектору.

Однією з важливих проблем банківської системи є непідготовленість переважної більшості банків до кризових явищ як на макро, так і на мікрорівні. Реалізовані державними органами заходи є недостатніми для зменшення наслідків фінансової кризи

Антикризове управлінням в банківському секторі слід розуміти як комплекс заходів, що дають системі можливість нейтралізувати дію дестабілізуючих чинників та повернути її в стан рівноваги, за умови коливань функціонування банківської системи в межах основних параметрів її стійкості і стабільності [13].

Метою антикризового управління банківською діяльністю на макрорівні є досягнення фінансової стабільності банківської системи. На макрорівні управлінські рішення спрямовуються на вирішення завдань: а) підтримка стабільності банківської системи України; б) забезпечення надійності системи гарантування вкладів фізичних осіб. Механізми участі держави в запобіганні банкрутству банківських установ слід дивесифікувати залежно від рівня проблемності ситуації та сценарію розвитку подій: криза одного банку, що не несе загрози банківській системі; криза групи банків, яка загрожує стабільності системи в регіональному масштабі чи в масштабах країни в цілому.

Метою антикризового управління на мікрорівні є досягнення фінансової стійкості окремої банківської установи. На мікрорівні завданням антикризового управління банком є: запобігання кризовим явищам; виведення банку з кризової ситуації, якщо не вдалося її уникнути, та відновлення роботи банку на докризовому рівні. Для виконання цих завдань система антикризового менеджменту має складатися з двох підсистем: прогнозування та запобігання кризі (діагностика); управління банком в умовах кризи (антикризові заходи та (або) реструктуризація). Відповідно до мети та завдань процес антикризового управління банком складається з етапів: діагностика та попередження кризових явищ; профілактичний етап; підготовчий етап; робота в умовах кризи [24].

Особливості функціонування банківської системи України на сучасному етапі характеризуються значними збитками банківських установ (понад 80 млрд. грн. станом на 01.01.2016 року), високими ризиками, що визначає необхідність формування значних резервів під активні операції, визнанням не платоспроможними великої кількості банків. Причини цих негативних явищ криються не тільки і не стільки у анексії Криму та військових діях на Донбасі, але значно глибші та є результатом прорахунків в управлінні державою загалом та фінансовим сектором зокрема у всі роки після здобуття незалежності.

Так, аналізуючи процеси становлення і розвитку вітчизняної банківської системи, можна виокремити чотири ключових причини виникнення не лише банківської кризи 2014-2016 років, а й попередніх банківських криз 1998, 2004, 2008-2009 років (рис. 1.18) [21].

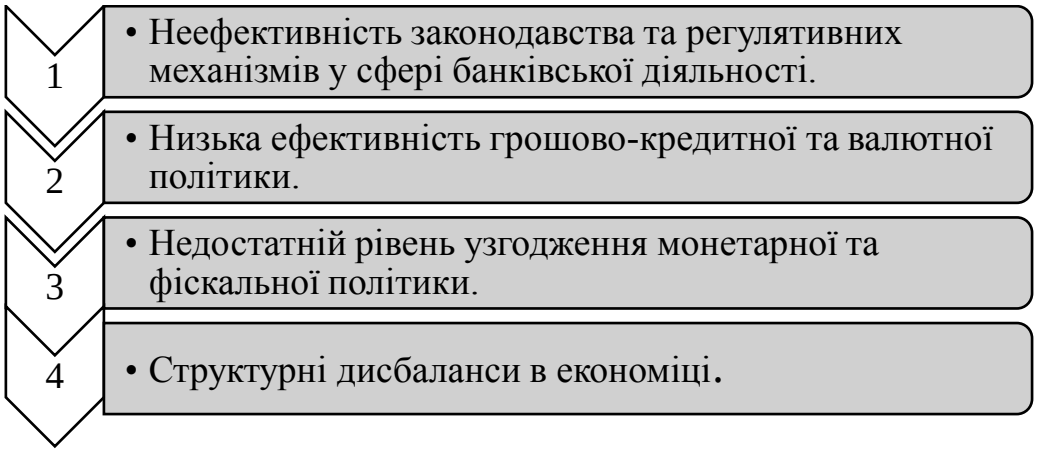


Рис. 1.18. Основні причини виникнення банківських криз

Джерело складено на автором на основі [29]

Варто більш детально розглянути кожний із них:

1. Не ефективність законодавства та регулятивних механізмів у сфері банківської діяльності. Виходячи з аналізу вітчизняного банківського законодавства, можна зробити висновок, що два найголовніші напрями діяльності комерційних банків (валютні операції та кредитування) практично нерегулюються на законодавчому рівні. В Україні валютні відносини регламентуються Декретом Кабінету Міністрів «Про систему валютного

регулювання і валютного контролю» від 19 лютого 1993 року, який є застарілим та регулює обмежене коло валютних відносин, а у сфері кредитування ще у 2004 році було скасовано єдине Положення НБУ «Про кредитування». За таких умов, починаючи із 2004 року в Україні різко зросла кредитна та депозитна доларизація, що в кінцевому підсумку призвело до зростання валютних ризиків, девальвації гривні та банкрутств підприємств і банків [16].

Відсутність дієвого законодавчого регулювання валютних відносин призводить до фактичної втрати Національним банком України контролю за емісійним механізмом, що ставить під сумнів його спроможність проводити самостійну грошово-кредитну політику та ефективно впливати за допомогою монетарних інструментів на реальний і фінансовий сектор економіки.

Щодо регулятивних механізмів, то, як показує практика, недостатньо ефективним є нагляд НБУ за цільовим використанням кредитів рефінансування. Також більшої ефективності потребують встановлені НБУ нормативи ліквідності та нормативи кредитних ризиків, адже в умовах кризи нормативи ліквідності завжди мають позитивне значення. Заниженими, на нашу думку, є і вимоги до мінімального розміру статутного капіталу, оскільки багато вітчизняних підприємств можуть одноосібно створити комерційний банк для кредитування власної діяльності, що згодом може призвести до його банкрутства [4].

2. Низька ефективність грошово-кредитної та валютної політики. Відсутність середньострокової стратегії реалізації грошово-кредитної та валютної політики створює проблеми для бізнес-планування діяльності комерційних банків на тривалу перспективу, а також не сприяє довірі до НБУ з боку економічних агентів. У кризовий період були відсутні нестандартні інструменти грошово-кредитного та валютного регулювання (такі як у ФРС США та ЄЦБ), що не сприяло забезпеченню оптимального рівня ліквідності банківської системи. Окрім цього, було суттєво підвищено облікову ставку Національного банку України до 30% в той час, коли інфляція була спричинена

не кредитним каналом монетарної трансмісії, а валютним каналом, що призвело до майже повного припинення банківського кредитування реального сектору економіки [11].

3. Недостатній рівень узгодження монетарної та фіскальної політики. У процесі реалізації державної економічної політики в Україні спостерігається неузгодженість дій НБУ та Уряду у сфері встановлення цілей макроекономічного регулювання, формування та прогнозування основних економічних параметрів розвитку, вирішення проблем капіталізації та ліквідації проблемних банків. розробки заходів щодо стимулювання розвитку національного виробництва, регулювання валютних відносин та вирівнювання платіжного балансу. За останній період монетарні інструменти набули невиправдано пріоритетного значення у дотриманні основних макроекономічних показників (валютний курс, інфляція, ВВП) порівняно із фіскально-бюджетними інструментами. Крім того, загрозливих розмірів почала набувати монетизація державного боргу, що фактично є шляхом до не контрольованої емісії [27].

4. Структурні дисбаланси в економіці. Практична відсутність реальних кроків державної економічної політики щодо подолання структурної розбалансованості економіки призводить до перманентної збитковості підприємств, надмірного рівня відкритості економіки, імпортом залежності країни, що негативно позначається на банківській діяльності створюючи кредитні та валютні ризики, підвищуючи вразливість національного господарства до глобальних економічних дисбалансів.

Подальша реструктуризація банківської системи України має бути спрямована на дві цілі: забезпечення стабільності її роботи та поступове підвищення ефективності. Для цього необхідно змінити механізм боротьби з ризиками у банківській системі: замість повального закриття банків необхідно створювати умови та сприяти їх злиттю та викупу інвесторами. Для цього необхідно змінити механізм боротьби з ризиками у банківській системі: замість повального закриття банків необхідно створювати умови та сприяти їх злиттю

та викупу інвесторами. Нехай цей шлях довший, але куди більш цивілізований та продуктивний. Виставлені вимоги до зростання власного капіталу із забезпеченням гарантій інвесторам, особливо іноземним, дозволять знизити ризики не руйнуючи довіру та без втрат власних коштів для юридичних та фізичних осіб.

Наступним моментом у механізмі реформування є повернення довіри до національної валюти і сприяння доларизації вкладів, що при аномальних стрибках курсу долара неможливе [10].

Очевидно, що на даний час вартість гривні щодо долара і євро через ситуацію на Сході країни, політичну напругу, економічну нестабільність суттєво занижена. В той же час, НБУ планує збільшити суми і частки депозитів у гривні до 80%, хоча механізм реалізації цих положень досі незрозумілий. Якщо і далі друкувати гроші для виплат Фондом гарантування вкладів, стабільності національної валюти не досягнути, а разом із тим і підвищення частки гривневих заощаджень.

Важливим кроком у реформуванні банківської системи має стати зменшення відсоткових ставок за депозитами і кредитами. НБУ в цьому напрямку планує затвердження відсотків на такому рівні:

– депозити (на рівні 3-4%);

– кредити (на рівні 7-8%).

Україна є однією країною з не багатьох, де ставки за депозитами сягають 20% - 25%. На основі ставок за депозитами можна простежити тенденцію відсоткових ставок кредитних продуктів. Адже, зазвичай, при великих відсотках на депозит, ставки за кредитами теж високі. Проте, високі ставки по депозитах – є лише яскравим свідченням нестачі пасивів для здійснення своєї діяльності, низьку платоспроможність і потребують негайного втручання основного регулятора банківської системи. Для порівняння, у США, Німеччині, Франції ставки по депозитах складають 0,5%, а по кредитах до 11-15%. Спостерігається значна різниця між відсотками на депозит і під кредит [25].

Крім цього, необхідно посилення як зовнішнього так і внутрішнього контролю над кредитними операціями. Необхідні вищі вимоги до позичальника, побудова нових якісно інших підходів до формування взаємовідносин з клієнтами. Банкам також доцільно відмовитися від стимулювання нераціональної економічної поведінки. Адже, якщо банк видає кредити на речі, які клієнту не по кишені, то в результаті постраждає і сам банк.

Щоб реалізувати реформи у кредитній і депозитній політиці банків необхідно на глобальному рівні:

– знизити ризик країни;

– знаходження надійного і дешевого джерела формування пасивів;

– підвищення суверенного рейтингу.

Стабільність і розвиток банківської системи залежить від розвитку реального сектору економіки.

Завершальною повинна стати реформа самої структури НБУ, а саме залучення під контроль НБУ: страхових компаній, ринку цінних паперів [2].

Таким чином, Національному банку України у тісній співпраці з Урядом необхідно вжити всіх можливих заходів щодо подолання зазначених вище проблем. В таблиці 1.16 запропоновані заходи подолання банківської та загально - економічної кризи в Україні

Таблиця 1.16

Заходи подолання банківських та загально - економічних криз в Україні

Сфера застосування	Заходи
у сфері валютної політики	обов’язкове отримання резидентами дозволів від органів валютного контролю на залучення іноземних кредитів чи на випуск зовнішніх позик; примусова конверсія позичок, отриманих на зовнішніх ринках в іноземній валюті, у національну валюту; депонування певної частини отриманих позичальником зовнішніх кредитів на спеціальних рахунках у центральному банку; посилення контролю за продажем цінних паперів нерезидентам і здійснення ними інвестицій; після стабілізації ситуації на валютному ринку та в економіці в цілому, доповнення Закону України «Про валютне регулювання і валютний контроль» нормами про заборону конверсійних операцій поза банками, обов’язкову конвертацію переказів фізичних осіб в національну валюту, заборону відкриття нових депозитів в іноземній валюті та внести зміни до Кримінального кодексу України

Сфера застосування	Заходи
	про кримінальну відповідальність за валютно-обмінні операції поза банками.
у сфері грошово-кредитної політи	відображення цілей грошово-кредитної та валютної політики у кількісному вираженні в Основних засадах грошово-кредитної політики; розробка рейтингу комерційних банків на основі проведення щоквартального стрес-тестування, відповідно до якого відбирати банки, які мають право отримувати кредити рефінансування; прийняття Закону України «Про банківське кредитування в Україні», в якому передбачити розділ «Умови, принципи та особливості кредитування Національним банком України комерційних банків», де чітко прописати: види і цілі кредитів рефінансування; вимоги до банків, які мають право і на основі яких критеріїв отримати кредит рефінансування; вимоги до застави за кредитами рефінансування; перелік санкцій та характер відповідальності за порушення цільового характеру кредиту рефінансування (внести відповідні зміни до Кодексу України про адміністративні правопорушення та Кримінального кодексу України; встановлення граничних лімітів (стель), які мають обмежити викуп Національним банком України ОВДП на первинному ринку з метою уникнення емісійного формування доходу Державного бюджету України; визначення розміру процентних ставок овернайт та процентних ставок за строковими кредитами рефінансування (які формуватимуть коридор ставок) на рівні базової ставки НБУ плюс/мінус 2-4процентних пункти.
у сфері банківського нагляду та контролю	законодавче закріплення вимоги щодо засновників банків, зокрема, один із засновників, що володіє часткою не менше 20%, повинен виступати гарантом надання фінансової допомоги у разі виникнення у банку фінансових труднощів. Інститут гаранта повинен діяти постійно, чим забезпечується відповідальність за результати діяльності банку та гарантія фінансової стійкості; удосконалення розрахунку нормативу адекватності регулятивного капіталу (Н2), де кредити підприємствам віднесені в шосту групу активів (ступінь ризику 100%) в частині ранжування ризиковості кредитів за фінансовим станом контрагентів; оптимізація розрахунку нормативів ліквідності в частині розрахунку нормативних значень загрупами банків за обсягом активів (найбільші, великі, середні та малі); удосконалення розрахунку нормативів кредитних ризиків шляхом внесення в базу розрахунку статті балансу комерційних банків «Інші фінансові активи»; підвищення ефективності управління ліквідністю банківської системи України через розгляд можливості створення на комерційній основі Фонду взаємодопомоги банкам під патронатом Асоціації українських банків та Українського кредитно-банківського союзу, що дозволить банкам оперативно залучати кошти для підтримки належного рівня ліквідності; впровадження механізму гарантування Національним банком України міжбанківських кредитів та виплат компенсацій у разі банкрутства банків-позичальників;
у сфері антиінфляційної політики:	тимчасова відмова Національного банку України від намірів застосування монетарного режиму інфляційного таргетування до часу створення належних передумов для ефективного інфляційного таргетування, зокрема: забезпечення високого рівня фінансової стійкості банківської системи; досягнення стабільних темпів економічного зростання; демонополізація економіки і відмова від адміністративного

Сфера застосування	Заходи
	контролю цін; забезпечення збалансованих доходів і витрат бюджету; розвиток внутрішнього споживання та імпортозаміщення; підвищення конкурентних переваг національного виробництва на зовнішніх ринках; забезпечення низького рівня доларизації економіки; забезпечення високогорівня незалежності центрального банку; зберегти певний перехідний період, напротязі якого потрібно здійснювати паралельне таргетування як інфляції, так і обмінного курсу.

Джерело складено автором на основі [15]

Крім того варто виділити фактори , які зумовлені кризою, що призвело до збільшення кількості злочинів, здіснених у банківській сфері:

- Економічна криза: призвела до погіршення фінансової ситуації в Україні: здешевлення національної валюти та занепад економічної сфери держави. Внаслідок цього погіршився фінансовий стан клієнтів. Внаслідок чого кредитори, щоб ухилитися від повернення коштів вдаються до порушення законодавства. На цьому фоні зустрічаються «злісні» шахраї, які мотивуючи власною неплатоспроможністю, уникають розрахунків з банками.

- Внаслідок передкризового активного кредитування населення – надання фіктивних довідок про прибутки. Такі дії вчинювалися з метою отримання кредиту при відсутності дійсної можливості виконати всі умови банку та побоювання позичальника за відмову у видачі кредиту при наявності «чесної» довідки.

- У період економічної кризи банки значно скоротили свої банківські продукти. Наслідком цього є збільшення зловживань з боку службових осіб банку, які за окрему плату допомагають клієнтам.

- Також значно збільшилась кількість шахрайств з майном, яке оформлене як застава під наданий кредит, - оформлюється зняття обтяження з нього на підставі фіктивних документів.

Тому, варто виділити основні вектори подальшого розвитку реструктуризації банківської системи України, які враховуватимуть інтереси населення України:

1. Припинення масового закриття банківських установ та перехід до політики їх об’єднання та поглинання шляхом застосування економічних важелів та стимулів.

2. Сприяння залученню іноземного капіталу в банківську систему України шляхом надання гарантій та створення сприятливого макросередовища.

3. Стимулювання повергнення довіри населення до банківської системи України шляхом підняття суми гарантування вкладів для нього (разом із зміною політики щодо проблемних банків це не призведе до збільшення суми виплат з ФГВФО).

4. Створення програми працевлаштування для працівників банків що залишились безробітними внаслідок масових банкрутств банків 2014-2015 років (включаючи працівників звільнених з самого НБУ внаслідок його реструктуризації).

Впровадження запропонованих заходів у сфері монетарної політики, банківського нагляду, кредитування реального сектору економіки дозволить відновити ефективну діяльність банківської системи України та сприятимуть економічній стабілізації.

Варто також розглянути особливості державного антикризового регулювання у банківському секторі України, які були здійснені з початком глобальної фінансової кризи з метою нейтралізації її негативного впливу [30].

1. Банки переглянули методики оцінки кредитоспроможності позичальників та запровадили жорсткіші умови кредитування.

2. НБУ вдвічі зменшив облікову ставку (з 15.06.2009 р. до 11% згідно з Постановою Правління НБУ “Про регулювання грошово-кредитного ринку” від 12.06.2009 р. № 343, та з 12.08.2009 р. до 10.25% згідно з Постановою Правління НБУ “Про зміну облікової ставки” від 10.08.2009 р. № 468). Із липня 2009 р. збільшено ставки обов’язкового резервування за короткостроковими ресурсами закордонного походження (з 4% до 20%). Ці заходи досить швидко призвели до подорожчання грошей на ринку (і депозитному, і кредитному), а

підвищення ставки резервування обмежило обсяги залучення валюти з-за кордону.

3. НБУ прийняв постанови “Про додаткові заходи щодо діяльності банків” від 11.10.2008 р. № 319 та “Про внесення змін до постанови Правління НБУ від 11.10.2008 р. № 319” від 16.10.2008 р. № 328, які обмежують обсяги надання кредитів юридичним і фізичним особам в іноземних валютах, забороняють рефінансування простроченої заборгованості шляхом видачі нових кредитів, а також необґрунтовану пролонгацію кредитів та внесення до кредитного договору змін щодо вартості кредиту, котрі не відповідають змінам облікової ставки НБУ.

4. Для стабілізації депозитного ринку та підтримання ліквідності НБУ запровадив мораторій на дострокове вилучення депозитів.

5. Знижено до 0% норму резервування на кошти, що залучаються на короткостроковій основі з іноземних джерел.

6. Дозволено враховувати в обов’язкових резервах касові залишки та державні облігації; активізовано заходи щодо рефінансування банків шляхом надання кредитів НБУ.

7. Для стабілізації валютного ринку та курсу гривні із середини жовтня 2008 року НБУ було вжито ряд заходів: почали здійснюватися регулярні валютні інтервенції НБУ (за три тижні було витрачено майже 5 млрд. доларів США золотовалютних запасів); для банків заборонено спекулятивні операції (купівля-продаж валют на міжбанківському ринку дозволялась лише за дорученням клієнтів та за їх курсом); курс продажу валют на готівковому ринку обмежувався офіційним курсом, а маржа банків від торгівлі валютами не повинна перевищувати 1.5%.

8. НБУ збільшив вартість власних кредитів, тобто вартість рефінансування на 0.5–1%.

9. Для розширення переліку банків, які можуть отримати кредити від НБУ, запропоновано рефінансування під заставу акцій банків. Але такі кредити зможуть отримувати лише ті банки, які дотримуються резервних вимог.

10. Згідно з Постановою Правління НБУ “Про внесення змін до Інструкції про порядок регулювання діяльності банків в Україні” від 17 грудня 2007 року № 458 запроваджено нову методику розрахунку адекватності банківського капіталу. Її мета – обмежити ризик розриву ліквідності, щоб уникнути наслідків ситуації, яка склалася на фінансовому ринку Сполучених Штатів Америки [22].

За даними рейтингового агентства Фітч Рейтингс (Fitch Ratings), запровадження нових регулятивних вимог щодо капіталу українських банків мало поліпшити їх кредитоспроможність. Такі заходи також повинні сприяти зменшенню доларизації економіки України та зростанню обсягів кредитування в національній валюті. Зазначимо, що рейтингове агентство Стандарт енд Пурс Рейтинг с Сервіс (Standard & Poor’s Ratings Services) знизило довгостроковий суверенний кредитний рейтинг України з “BB–” до “B+” з огляду на підвищення інфляційних очікувань, велику зовнішню заборгованість вітчизняних комерційних банків, зростання дефіциту поточного рахунку платіжного балансу та інші негативні чинники.

В плив банківської кризи на загальноекономічну активність, фінансову стійкість і безпеку банківської системи та країни в цілому зумовлює необхідність розробки алгоритму аналізу банківських криз як основи для моніторингу банківської системи на чутливість до зовнішніх шоків та застосування системних заходів з їх подолання. Алгоритм моніторингу стійкості банківської системи відображено на рис. 4

Крім того, специфічні властивості діагностики мають бути враховані в антикризовому управлінні і включати:

– вивчення нових властивостей розвитку банку як об’єкта управління в результаті розвитку фінансової і банківської систем;

– виявлення причинно-наслідкових зв’язків у розвитку об’єктів і суб’єктів банківської системи;

– визначення граничних меж експертної компетенції менеджера й експертних систем, що використовуються в діагностиці кризи, її попередження і виходу з неї;

– моніторинг зміни ситуації у банківській сфері в умовах кризових явищ;

– підвищення ефективності антикризових і прогностичних функцій діагностики.

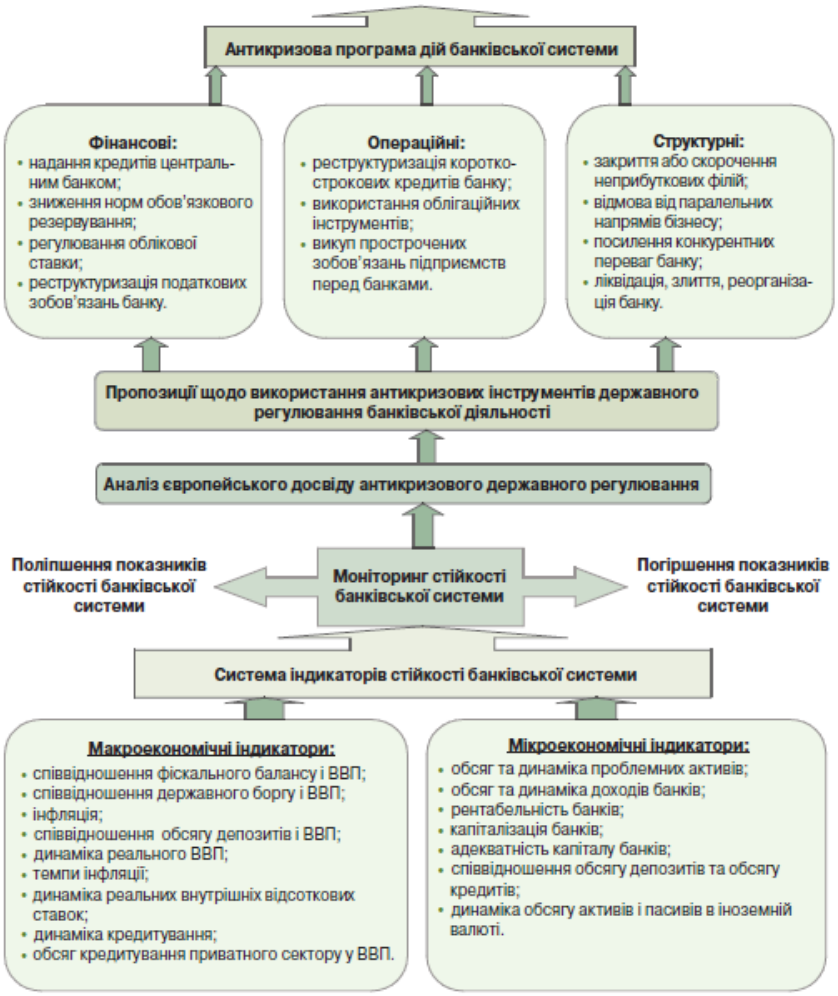


Рис. 1.19. Алгоритм моніторингу стійкості банківської системи України

Джерело складено автором на основі [12]

Даний алгоритм моніторингу стійкості банківської системи дає змогу оцінити розвиток банківської системи України з урахуванням макро- і мікро-особливостей, що, в свою чергу, дає підстави до визначення антикризових заходів та вироблення рекомендацій з коригування політики для посилення стійкості банківської системи та запобігання фінансовим кризам.

На підставі проведеного дослідження можна надати низку рекомендацій щодо вдосконалення механізму регулювання банківської діяльності в Україні у кризових умовах, а саме:

- провести ретельний аналіз причин виникнення глобальної фінансової кризи та глибини її впливу на світову економіку;
- змоделювати поведінку внутрішнього фінансового ринку в умовах уже діючих антикризових заходів НБУ та уряду хоча б на найближчу перспективу;
- сформувати антикризову програму дій банку, яка має бути за характером короткостроковою, гнучкою та відкритою для коригування;
- проводити реструктуризацію проблемних кредитів за єдиними для всіх банків правилами, розробленими регулятором, під його контролем та за його підтримки. При цьому важливо враховувати специфіку і пріоритети кожного з таких кредитів: за категорією позичальника (фізичні, юридичні особи), за цільовим призначенням (іпотечні, автокредити, кредити підприємцям, споживчі, корпоративні кредити, міжбанківські позики); за видом валюти (національна, іноземна); за ступенем проблемності (стандартні, під контролем, субстандартні, сумнівні, безнадійні); за строками погашення тощо;
- запровадити контроль за максимальним розміром оплати процедури реструктуризації та обмеження на встановлення нових вимог до забезпечення за кредитом (переоцінки заставного майна, вимоги додаткового забезпечення тощо). Збитки, пов’язані з реструктуризацією, обов’язково повинні розподілятися між банками, позичальниками та державою;
- вдосконалити методику класифікації проблемних кредитів, розробити порядок викупу та обслуговування проблемних активів;
- створити госпітальну фінансову установу змішаної форми власності з державним контрольним пакетом. Завдяки цьому зменшується навантаження на держбюджет, і водночас за державою залишається контроль за процедурою викупу та реструктуризації активів. При цьому розподіл повноважень різних власників можливо передбачити установчими документами госпітальної установи. Одним із варіантів такого розподілу може бути участь держави у

реструктуризації найпроблемніших позик населення та можливість їх викупу за рахунок бюджету. Рештою проблемних банківських активів опікуються підрозділи госпітальної установи, що фінансуються з інших джерел, зокрема, за рахунок коштів засновників – приватних осіб. Узагалі, було б ідеальним, якби організаційна структура госпітальної установи відповідала характеру проблемності викуплених активів;

- необхідно, щоб оцінку вартості проблемних активів за методикою НБУ виконувала третя, незалежна сторона;

- кожен банк має внести радикальні зміни до системи управління бізнесом – і не лише тактичного, а й стратегічного характеру. Якщо за стабільних умов золотим правилом банківського менеджера є “максимізація прибутку за дотримання ліквідності та прийнятного рівня ризику”, то в кризових умовах на перший план повинна виходити система управління ризиками. Це дасть змогу максимально захиститися від впливу фінансової кризи та мінімізувати втрати;

- нарощувати офіційні валютні резерви відповідно до зростання валового зовнішнього боргу для забезпечення стійкого розвитку економіки та обмеження впливу зовнішніх факторів. Використовуючи механізм перекредитування в умовах світової кризи ліквідності, банки можуть зіткнутися з проблемою нестачі коштів для покриття короткострокових зобов’язань. Тому органам контролю треба приділити більше уваги обмеженню розривів у термінах запозичення та розміщення коштів комерційними банками, адже активні операції характеризуються довшими термінами, ніж пасивні;

- використовувати фінансові інструменти грошово-кредитного регулювання для підвищення ефективності монетарної політики в державі та структурні інструменти для оптимізації внутрішньої та зовнішньої структур фінансово-кредитних установ як основних учасників фінансового сектору, котрі безпосередньо впливають на рівень його стійкості і надійності;

- застосовувати операційні інструменти шляхом удосконалення внутрішнього моніторингу структури активів та зобов’язань банківських

установ як основного чинника запоруки безпеки клієнтської бази та стабільності функціонування реального сектору економіки.

Банківська система – одна з найголовніших ланок економічної системи країни, і будь-яка загроза стабільності банків завдає шкоди всій економіці, добробуту кожного громадянина. Тому під час кризи центральні банки та уряди провідних країн світу не шкодують коштів і вживають безпрецедентних заходів, аби підтримати свої банківські системи [7].

З метою нейтралізації впливу глобальної фінансової кризи в Україні використовувалися різні інструменти державного антикризового регулювання банківського сектору (банки переглянули методики оцінки кредитоспроможності позичальників та запровадили жорсткіші умови кредитування; НБУ ввів мораторій на дострокове вилучення депозитів тощо).

Водночас доцільно вжити додаткових заходів:

- внести необхідні зміни до законодавства (передусім банківського і податкового);
- вдосконалити методику класифікації проблемних кредитів;
- розробити порядок викупу та обслуговування проблемних активів, методику оцінки їх вартості й інші необхідні положення;
- вдосконалити систему управління ризиками, зокрема, кредитними;
- забезпечити нарощування офіційних валютних резервів відповідно до зростання валового зовнішнього боргу з метою сприяння стійкому розвитку економіки та обмеженню впливу зовнішніх факторів.

Розроблений алгоритм моніторингу стійкості банківської системи, дасть змогу оцінити розвиток банківської системи України з урахуванням макро- і мікро- особливостей, що слугуватиме підставою для визначення антикризових заходів та вироблення рекомендацій з коригування регуляторної політики, що сприятиме зміцненню стійкості банківської системи та упереджуватиме фінансові кризи.

Таким чином, очевидно, що банківська система знаходиться у зоні підвищеного ризику. Це обумовлюється тим, що практично вся банківська

діяльність, починаючи від оформлення кредиту, і закінчуючи інкасацією грошових коштів, є досить ризикованою. Значна кількість як зовнішніх, так і внутрішніх загроз можуть завдати роботі банку, його співробінникам та клієнтам суттєвих втрат. За умов, що склалися, банки повинні систематично відстежувати наявність усіх видів загроз, вивчати можливості та шляхи їх попередження, вживати всіх можливих заходів щодо їх локалізації та нейтралізації шкідливих наслідків. Про те, банківська система України має всі передумови, щоб пережити вплив глобальної фінансової кризи.

Список використаних джерел:

1. *Афанасьєва О. Б. Антикризове регулювання діяльності банків в Україні в період світової фінансової кризи / О. Б. Афанасьєва // Соціально-економічні проблеми сучасного періоду України. Фінансовий ринок України: стабілізація та євроінтеграція : зб. наук. праць. – Львів, 2010. – Вип. 1 (81). – С. 316-325.*
2. *Барановський О.І. Фінансові кризи: передумови, наслідки і шляхи запобігання : монографія / О.І. Барановський. – К. : Київ. нац. торг.-екон. ун-т, 2009. – 754 с.*
3. *Барановський О. Проблемні банки : виявлення й лікування / О. Барановський // Вісн. Нац. банку України. — 2009. — № 11. — С. 18–31.*
4. *Барановський О.І. Банківська безпека: проблема виміру // Економіка і прогнозування. – 2006. – № 1. – С.7-26.*
5. *Вольниченко В. Гроші та економіка / В. Вольниченко // Тиждень: Всеукраїнський тижневик. – 2008. – № 2. – С. 2-3.*
6. *Вовк В. Я. Концептуальні засади формування організаційно-економічного механізму антикризового управління банком / О. М. Тридід, В. Я. Вовк // Фінанси України. – 2009. – № 1. – С. 98-106.*
7. *Горохова О. Антикризове регулювання банківської сфери як умова фінансово-економічної стабільності / О. Горохова, В. Лагутін // Менеджмент та маркетинг в бізнесі XXI століття. – 2008. – № 18. – Т. 2. – С. 31-36.*
8. *Дзюблюк О. Грошово-кредитна політика в період кризових явищ на світових фінансових ринках / О. Дзюблюк // Вісник НБУ. – 2012. - № 5. – С. 20 – 30.*
9. *Данилов Р.І. Антикризове управління ресурсами комерційних банків [Електронний ресурс] / Р. І. Данилов, С. О. Мормуль // Сьома Всеукраїнська науково-практична інтернет-конференція "Сучасний соціокультурний простір 2010". – Режим доступу: http://intkonf.org/danilov-komertsiynih-bankiv.*
10. *Дмитров С.О. Фінансовий моніторинг в банку: Навчальний посібник / С.О. Дмитров, В.В. Коваленко, А.В. Єжов, О.М. Бережний; За ред. С.О. Дмитрова, В.В. Коваленко. – Суми: ВТД «Університетська книга», 2013. – 336 с.*
11. *Захаров В. Я. Антикризисное управление. Теория и практика : учеб. пособ. для студентов вузов, обучающихся по специальностям экономики и управления / Захаров В. Я., Блинов А. О., Хавин Д. В. – М. : ЮНИТИ–ДАНА, 2006. – 287 с.*
12. *Зарицька І.М. Передумови та особливості прояву сучасної світової банківської кризи // Вісник НБУ. – 2009. – № 6 (160). – С. 20-29.*
13. *Кузнєцова Л.В. Вплив глобалізації на розвиток банківської діяльності. Кол. монографія. – Одеса: Видавництво "Атлант", 2011. – 520 с.*
14. *Котенко О.О. Напрямки впровадження елементів антикризового управління в комерційних банках України [Електронний ресурс] / О. О. Котенко // Сьома Всеукраїнська*

науково-практична інтернет-конференція "Сучасний соціокультурний простір 2010".– Режим доступу: http://intkonf.org/antikrizovogoupravlinnya- v-komertsiynih-bankah-ukrayini.
15. Костогриз В. Аспекти антикризового управління банківською діяльністю в Україні / В. Костогриз // Економічний аналіз. – 2010. – №7. – С. 156-158.
16. Коваленко В. Інструменти державного антикризового управління в банківському секторі / В. Коваленко // Вісник Української академії банківської справи. – 2006.– № 2. – С. 8-14.
17. Коваленко В.В. Антикризове управління в забезпеченні фінансової стійкості банківської системи : [монографія] / В. В. Коваленко, О. В. Крухмаль. – Суми: УАБС НБУ, 2007. – 198 с.
18. Клюско Л.А. Антикризовий банківський менеджмент як інструмент управління економічною безпекою кредитних установ // Науковий вісник Львівського державного університету внутрішніх справ. Серія "Економіка". – 2009. – Випуск 2. – С. 269-278.
19. Ковзанадзе И.К. Роль денежно-кредитной политики в преодолении последствий банковских кризисов // Деньги и кредит. – 2003. – № 2. – С. 45-47.
20. Коваленко В. В. Стратегічне управління фінансовою стійкістю банківської системи: методологія і практика [Текст] : монографія / В. В. Коваленко. - Суми : ДВНЗ ЇУАБС НБУ, 2010. – 228 с. - ISBN 978-966-8958-65-6.
21. Мескон М.Х., Альберт М. Хедоури Ф. Основы менеджмента: Пер. с анг. – М.:Дело, 2014. – 702с.
22. Мельник А.О. Теоретичні підходи висвітлення фінансових криз / А.О. Мельник // Наука й економіка – 2009. – № 4 (16), Т. 1. – С. 106-110.
23. Олійник А.А. Напрями оптимізації ресурсного портфелю банків України / А.А. Олійник // Тенденції розвитку економіки у 2014 році: аналітичний та теоретико-методологічний аспекти: матеріали Міжнародної науково-практичної конференції. – 2014. – № 1. – С. 52–54.
24. Пернарівський О.В. Аналіз, оцінка та способи зниження банківських ризиків // Вісник НБУ. – 2004. – № 4. – С. 44-48.
25. Смовженко Т. С. Антикризове управління стратегічним розвитком банку: монографія / Т. С. Смовженко, О. М. Тридід – Київ: УБС НБУ, 2008. – 473 с.
26. Стельмах В.С., Міщенко В.І., Крилова В.В., Набок Р.М., Приходько О.Г., Грищук Н.В. Ліквідність банку : окремі аспекти управління та світовий досвід регулювання і нагляду : Науково–аналітичні матеріали. Вип. 11 / – К. : Національний банк України. Центр наукових досліджень. – 2008. – 220 с.
27. Степаненко А. Деякі аспекти антикризового управління банківською системою // Вісник КНТЕУ. – 2008. – № 3. – С. 77-84.
28. Терещенко О. О. Антикризове фінансове управління на підприємстві : vонографія / О. О. Терещенко, Г. М. Пухтаєвич. – 2–ге вид., без змін. – К. : КНЕУ, 2006. – 268 с.
29. Терещенко О. О. Антикризове фінансове управління на підприємстві : vонографія / О. О. Терещенко, Г. М. Пухтаєвич. – 2–ге вид., без змін. – К. : КНЕУ, 2006. – 268 с.
30. Тарасова О.В., Панова Ю.О. Стан і тенденції розвитку банківської системи України. // Економіка харчової промисловості.- 2014.-№ 3(23). - С. 79-86.
31. Тавасиев А. М. Антикризисное управление кредитными организациями: [учеб. пособ.] / Тавасиев А. М. – М: ЮНИТЫ-ДАНА, 2014. – 480 с.

РОЗДІЛ 2
МЕХАНІЗМИ ПРОТИДІЇ ЗЛОЧИНАМ В ЕКОНОМІЧНІЙ СФЕРІ

2.1. НАПРЯМИ УДОСКОНАЛЕННЯ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ БУДІВЕЛЬНИХ ПІДПРИЄМСТВ ДЛЯ ЗАПОБІГАННЯ ЗЛОЧИНАМ У ЕКОНОМІЧНІЙ СФЕРІ

ДМИТРЕНКО ВАСИЛЬ ІВАНОВИЧ*, к.е.н.,*
ЧЕРЕВКО ОЛЕКСАНДР ВОЛОДИМИРОВИЧ, *д.е.н., професор,*
професор кафедри менеджменту та економічної безпеки,
Черкаський національний університет імені Богдана Хмельницького

Основною метою формування організаційно-економічного механізму підприємства будівельної галузі є забезпечення сприятливих економічних та організаційних умов для його діяльності, розвитку, швидкого відновлення потенціалу підприємства.

Проведене дослідження сучасних підходів до трактування понять «механізм», «механізм державного регулювання» та «система економічної безпеки будівельних підприємств», а також встановлення специфіки діяльності будівельних підприємств, зумовили необхідність авторського трактування поняття «механізм державного регулювання системи економічної безпеки будівельних підприємств» як сукупність організаційних, управлінських, соціальних та технологічних заходів впливу державного регулювання на процес будівництва з метою забезпечення економічної безпеки будівельного підприємства.

До *основних елементів* механізму державного регулювання системи економічної безпеки будівельних підприємств пропонуємо віднести:

– об’єкти та суб’єкти державного регулювання системи економічної безпеки будівельних підприємств;

– функції державного регулювання системи економічної безпеки будівельних підприємств;

– сукупність принципів, які забезпечують функціонування механізму державного регулювання системи економічної безпеки будівельних підприємств під впливом державного регулювання;

– основні складові механізму державного регулювання системи економічної безпеки будівельних підприємств;

– важелі впливу державного регулювання на систему економічної безпеки будівельних підприємств (рис. 2.1).

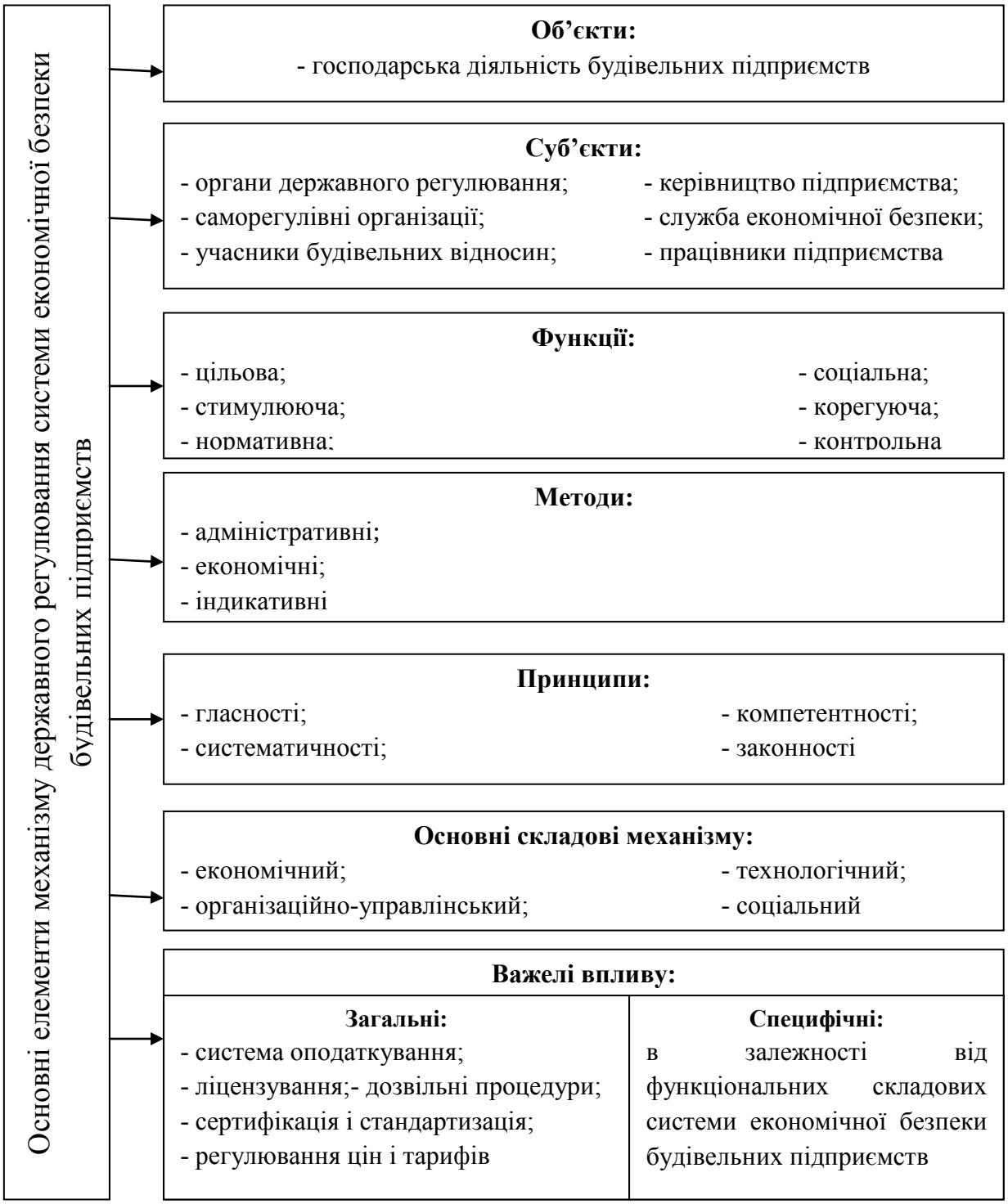


Рис. 2.1. Основні елементи механізму державного регулювання системи економічної безпеки будівельних підприємств

Складено особисто автором

До основних об’єктів державного регулювання системи економічної безпеки будівельних підприємств пропонуємо віднести всю господарську діяльність будівельних підприємств.

Серед основних суб’єктів механізму державного регулювання системи економічної безпеки будівельних підприємств пропонуємо назвати органи державного регулювання, саморегулівні організації у сфері будівництва, підприємства-учасники будівельних відносин, керівництво, служби їх економічної безпеки та працівників будівельних підприємств (рис. 2.2).

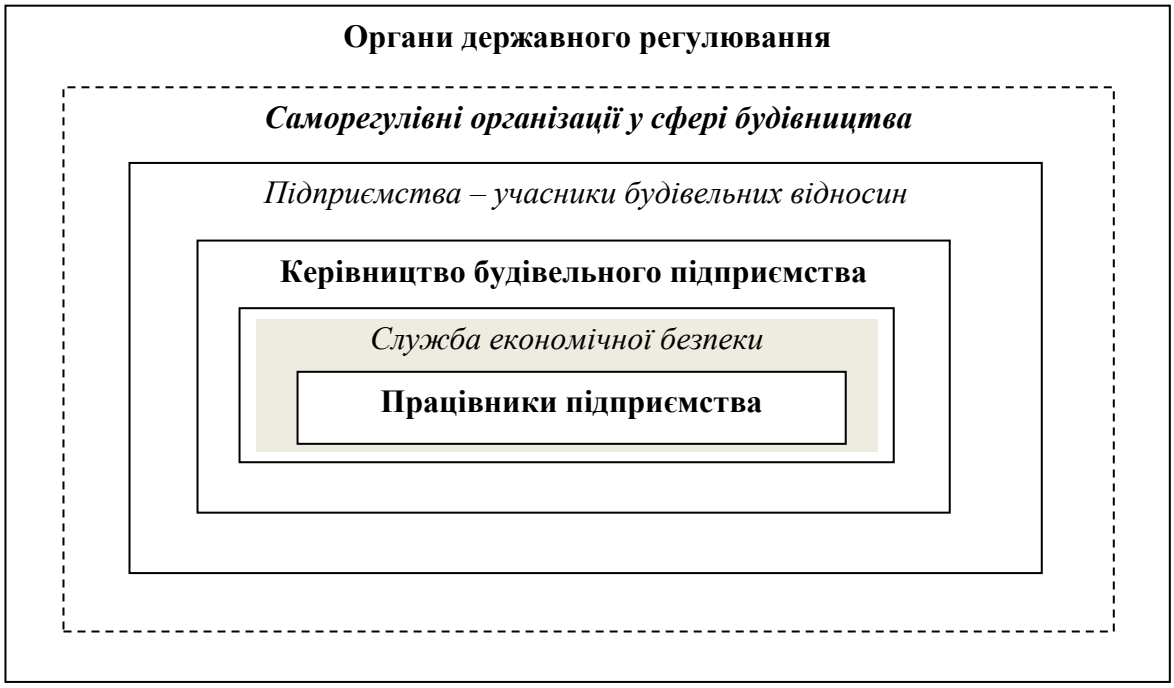


Рис. 2.2. Суб’єкти механізму державного регулювання системи економічної безпеки будівельних підприємств

Джерело: доопрацьовано автором на основі [1]

На рис. 2.2 суцільною лінією позначено прямий вплив суб’єктів системи, а пунктиром – непрямий вплив суб’єктів системи економічної безпеки будівельних підприємств.

На наш погляд, саме ієрархічний підхід до групування суб’єктів системи економічної безпеки будівельних підприємств дозволить встановити ступінь впливу кожного із зазначених суб’єктів та з’ясувати роль держави в її забезпеченні.

До основних функцій державного регулювання системи економічної безпеки будівельних підприємств пропонуємо віднести наступні*:*

- цільова – така функція має дуалістичних характер, оскільки, з одного боку, регламентує цільове використання коштів в процесі будівництва, а, з іншого, - отримання ліцензій та дозволів на окремі види будівельних робіт;

- стимулююча – більш чітко регламентуючи вимоги до кадрового, технічного, інформаційного та інших видів забезпечення процесу будівництва, підвищує рівень конкурентоспроможності будівельних підприємств;

- нормативна – передбачає наявність та неухильне виконання нормативів на різних етапах будівельної діяльності;

- соціальна – встановлюючи нормативи по оплаті праці, дозволяє підвищувати рівень соціального захисту працівників будівельних підприємств;

- корегуюча – передбачає юридичне коригування вартості будівельних послуг, що забезпечує фінансову стійкість будівельних підприємств, позитивно впливаючи на їх економічну безпеку;

- контрольна – наявність контрольних заходів на всіх етапах будівництва дозволяє знизити ризик від невідповідного їх виконання, що забезпечує належний стан системи економічної безпеки будівельних підприємств.

До основних методів державного регулювання системи економічної безпеки будівельних підприємств пропонуємо віднести наступні:

- адміністративні – передбачають наявність методів регламентування діяльності будівельних підприємств у сфері кадрового, інформаційного, документаційного та інших видів забезпечення, що дозволяють регулювати стан системи економічної безпеки будівельних підприємств;

- економічні – передбачають встановлення нормативів у сфері ціноутворення, оплати праці, оподаткування, вартості ліцензій та дозволів тощо, що дозволяють регулювати стан системи економічної безпеки будівельних підприємств;

- індикативні – характеризують наявність індикаторів за якими встановлюється стан системи економічної безпеки будівельних підприємств.

В основі механізму державного регулювання закладені певні принципи і чітке дотримання їх при здійсненні контрольної діяльності незалежно від того, щодо кого або чого вона здійснюється.

Принцип гласності державного регулювання передбачає не лише виявлення недоліків та обов'язкове покарання, а й постановку актуальних проблем, обговорення проектів управлінських рішень, підготовку громадської думки.

При здійсненні державного регулювання необхідно дотримуватися *принципу систематичності*, регулярності щодо його проведення. Це вносить певний порядок і дисципліну в роботу як того, кого контролюють, так і того, хто контролює. До того ж систематичний контроль дає змогу краще орієнтуватися в конкретній галузі управління та постійно аналізувати стан справ, а також виявляти недоліки в управлінській діяльності, відшукувати резерви чи запобігати непередбаченим наслідкам.

Принцип компетентності державного регулювання передбачає високий рівень кваліфікації працівників як будівельних підприємств, так і контролюючих органів, для підвищення ефективності та позитивного впливу на досягнення результату діяльності.

Принцип законності державного регулювання передбачає високий рівень регламентації процесу будівництва на всіх його етапах від початку до здачі об'єктів у експлуатацію.

Основними складовими механізму державного регулювання системи економічної безпеки будівельних підприємств пропонуємо вважати наступні: економічний механізм, організаційно-управлінський механізм, соціальний механізм та технологічний механізм (рис. 2.3) [2].

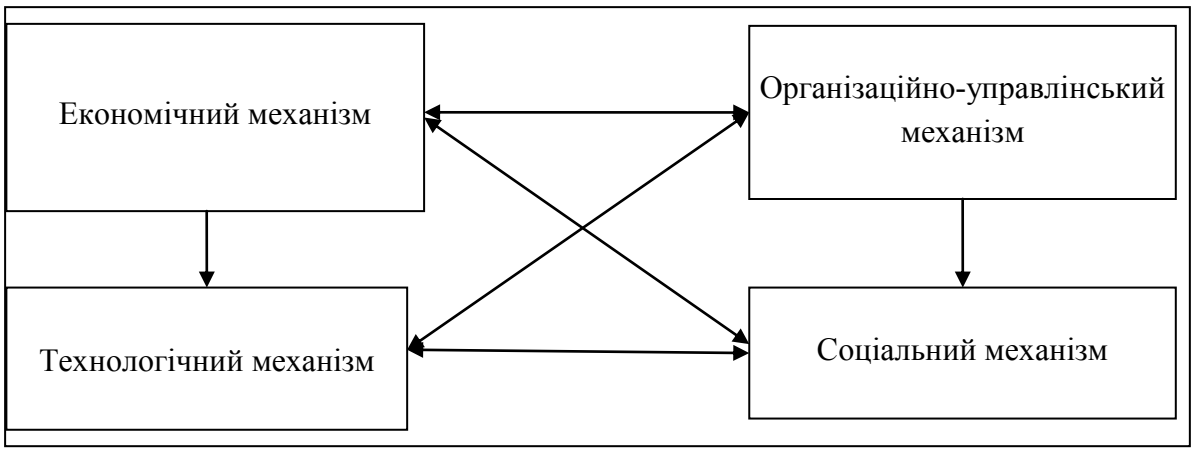


Рис. 2.3. Основні складові механізму державного регулювання системи економічної безпеки будівельних підприємств

Складено особисто автором

При здійсненні державного регулювання системи економічної безпеки будівельних підприємств головну роль відіграє *економічний механізм*, який відповідає за фінансове забезпечення, здійснює контроль та оцінку ефективності окремих будівельних підприємств та будівельної галузі в цілому.

Динамічний та статичний характер економічного та організаційного механізму в сукупності реалізує функцію управлінського впливу. Тому даний взаємозв'язок пропонуємо розглядати як *організаційно-управлінський механізм* державного регулювання системи економічної безпеки будівельних підприємств.

Соціальний механізм державного регулювання системи економічної безпеки будівельних підприємств забезпечує виконання завдання розвитку трудових відносин, нарощуванню інтелектуального капіталу, збільшення продуктивності праці та покращення якості праці за допомогою мотиваційних заходів.

Технологічний механізм як частина механізму державного регулювання системи економічної безпеки будівельних підприємств характеризує саме специфіку даного виду діяльності та вказує на відповідні особливості її здійснення, а саме: ліцензуванні будівельної діяльності, виконанні робіт підрядника, виконанні ролі замовника будівельних робіт тощо.

Основні етапи формування та функціонування механізму державного регулювання системи економічної безпеки будівельних підприємств наведено на рис. 2.4.

Рис. 2.4. Основні етапи формування та функціонування механізму державного регулювання системи економічної безпеки будівельних підприємств

Складено особисто автором

Основні важелі впливу державного регулювання системи економічної безпеки будівельних підприємств пропонуємо розподілити на дві групи:

1) загальні**:**

- система оподаткування;
- ліцензування;
- дозвільні процедури;
- державне замовлення;
- сертифікація і стандартизація;
- регулювання цін і тарифів;

2) специфічні (в залежності від функціональних складових системи економічної безпеки будівельних підприємств):

1. *У сфері кадрової безпеки.* З метою покращення кадрової безпеки в органах Державної архітектурно-будівельної інспекції (далі – ДАБІ) України та її територіальних органах пропонуємо розробити та затвердити порядок заміщення вакантних посад в ДАБІ України та її територіальних підрозділах. Метою такого порядку є призначення на посади в органи державного архітектурно-будівельного контролю найбільш досвідчених фахівців.

Основним інструментом перевірки працівників може стати незалежне комп'ютерне тестування, яке пропонуємо проводити за двома напрямами:

1) перевірка особистих якостей (на поліграфі);

2) перевірка професійних якостей (на професійних тестах).

Основним завданням порядку є зменшення впливу людського фактору при відборі кадрів, зокрема керівництва органів ДАБІ України та її територіальних органів.

Пропонуємо розробити та впровадити кваліфікаційні вимоги до осіб, які претендують на зайняття посад державних службовців в органах державного архітектурно-будівельного контролю України. Кваліфікаційні вимоги, окрім основних критеріїв, яким повинні відповідати претенденти на заміщення посад державних службовців відповідно до чинного законодавства, повинні мати відповідні фахові вимоги, зокрема вищу освіту в галузі будівництва

(архітектура, будівництво, виробництво будівельних матеріалів) для посад головних державних інспекторів, керівників та заступників керівників підрозділів по контролю за будівництвом, вищу освіту в галузі юриспруденції для посадових осіб юридичних підрозділів.

Керівники ДАБІ України, територіальних органів та їх заступники повинні мати вищу освіту також з державного управління. Особи, що претендують на заміщення вакантних посад в органах ДАБІ України повинні мати стаж роботи за фахом або державної служби відповідно до рівня посад, на зайняття яких претендують.

Також необхідно розробити та впровадити порядок просування по службі посадових осіб органів державного архітектурно-будівельного контролю. Ротація керівних кадрів (керівників та заступників керівників територіальних органів) має здійснюватися кожні п’ять років за наказом голови ДАБІ України з метою недопущення зрощування з будівельними підприємствами та зниження рівня виникнення корупційних загроз.

2. *У сфері інформаційної безпеки.* З метою покращення рівня внутрішньо комунікаційних зв’язків необхідно розробити та впровадити в системі органів ДАБІ України єдиний порядок накопичення, збирання та обміну службовою інформацією з питань здійснення державного архітектурно-будівельного контролю. Порядок має нормативно встановити механізми взаємодії між структурними підрозділами, посадовими особами органів ДАБІ України, механізми обміну інформацією з питань здійснення державного архітектурно-будівельного контролю. Разом з таким порядком мають бути передбачені шляхи захисту службової та конфіденційної інформації будівельних підприємств, передбачена відповідальність за порушення вказаного порядку працівниками ДАБІ згідно із законодавством, що в свою чергу також позитивно вплине на стан економічної безпеки і будівельних підприємств.

3. *У сфері інтерфейсної безпеки.* Для покращення зовнішньо комунікаційних зв’язків необхідно розробити та впровадити нормативний документ, який надасть роз’яснення будівельним підприємствам щодо

інформації, яка повинна буде ними оприлюднена на всіх етапах будівельних робіт саме і Інтернет-мережі та засобах масової інформації. Такий документ допоможе, з одного боку, привести у відповідність всі сайти будівельних підприємств, а з іншого – дозволить інвесторам слідкувати за процесом будівництва, що покращить стан економічної безпеки всіх учасників будівельних відносин.

4. *У сфері фінансової безпеки.* Покращенню структури органів державного архітектурно-будівельного контролю має сприяти модернізація Державної архітектурно-будівельної інспекції України шляхом повного структурного та господарського підпорядкування територіальних органів державного архітектурно-будівельного контролю Державній архітектурно-будівельній інспекції України. У зв'язку з цим буде здійснено перерозподіл фінансових потоків за отримані ліцензії та дозволи, що також певною мірою вплине на стан системи економічної безпеки будівельних підприємств.

5. *У сфері правової безпеки.* В структурі органів державного контролю доцільно створити підрозділ контрольних перевірок ДАБІ України, розробити та затвердити положення про управління контрольних перевірок, згідно якого основним завданням вказаного підрозділу мають бути планові перевірки поточної діяльності територіальних органів ДАБІ України, органів державної влади та місцевого самоврядування на предмет дотримання містобудівного законодавства та здійснення позапланових перевірок за зверненням центральних органів державної влади, правоохоронних органів вищого рівня (Генеральної Прокуратури України, Міністерства Внутрішніх Справ України, Служби Безпеки України, Антикорупційного бюро тощо).

Основним завданням вказаного підрозділу має бути профілактика та протидія корупційним злочинам, адміністративним корупційним порушенням з боку осіб, віднесених до суб'єктів відповідальності за корупційні правопорушення при здійсненні державного архітектурно-будівельного контролю. Вказаний підрозділ повинен взаємодіяти з правоохоронними органами стосовно профілактики та протидії корупції в системі державного

архітектурно-будівельного контролю. Підрозділу необхідно надати повноваження здійснювати службові перевірки за наказом голови або заступника голови ДАБІ України з питань запобігання та протидії корупції в системі державного архітектурно-будівельного контролю.

6. *У сфері технологічної безпеки.* З метою покращення обізнаності працівників органів ДАБІ України, пропонуємо зобов’язати їх проходити підвищення кваліфікації та стажування на діючих будівельних підприємствах України та за кордоном. Набутий досвід буде корисний як з метою удосконалення самого процесі державного регулювання, так і для практичної обізнаності працівників.

Таким чином, необхідною передумовою розвитку й удосконалення механізму державного регулювання системи економічної безпеки будівельних підприємств є впровадження комплексу заходів, спрямованих на покращення кадрової, правової, фінансової, інформаційної, інтерфейсної та технологічної складових системи економічної безпеки будівельних підприємств.

Розвиток механізму державного регулювання системи економічної безпеки будівельних підприємств дозволить покращити ефективність функціонування відповідних державних органів, внаслідок чого має підвищитися рівень економічної безпеки будівельних підприємств та всіх учасників будівельних відносин в цілому.

Вдосконалення системи економічної безпеки будівельних підприємств повинно враховувати сукупність об'єктивних і суб'єктивних чинників, які визначають специфіку діяльності саме будівельних підприємств, в тому числі впливу державного регулювання на їх діяльність.

В основу вдосконаленої системи економічної безпеки будівельних підприємств, покладений системно-структурний підхід, який передбачає урахування різних елементів і складових, що характеризують економічну систему будівельного підприємства. Системно-структурний підхід передбачає, що вдосконалення системи економічної безпеки будівельних підприємств

повинно починатись з формування загальної концепції економічної безпеки. Така концепція повинна ураховувати наступні складові (рис. 3.4):

1) мету та завдання функціонування системи економічної безпеки будівельних підприємств;

2) принципи функціонування системи економічної безпеки будівельних підприємств;

3) встановлення основних загроз, які впливають на систему економічної безпеки будівельних підприємств;

4) методичний підхід до оцінювання стану системи економічної безпеки будівельних підприємств;

5) напрями вдосконалення функціонування системи економічної безпеки будівельних підприємств.

Пропонуємо вважати основною метою функціонування системи економічної безпеки будівельного підприємства мінімізацію впливу внутрішніх та зовнішніх загроз діяльності будівельних підприємств під впливом державного регулювання.

Мета функціонування системи економічної безпеки реалізується за рахунок низки завдань, серед яких найважливішими є:

- розробка нормативно-правового забезпечення функціонування системи економічної безпеки будівельних підприємств;

- систематизація суб’єктів системи економічної безпеки будівельних підприємств;

- ідентифікація основних загроз діяльності будівельних підприємств під впливом державного регулювання;

- розробка методичного підходу до оцінювання стану системи економічної безпеки будівельних підприємств.

Основними принципами організації системи економічної безпеки будівельних підприємств є наступні: наукової обґрунтованості, стратегічної орієнтації, цільової спрямованості, інформаційної прозорості, гласності, конфіденційності, постійності, підзвітності.

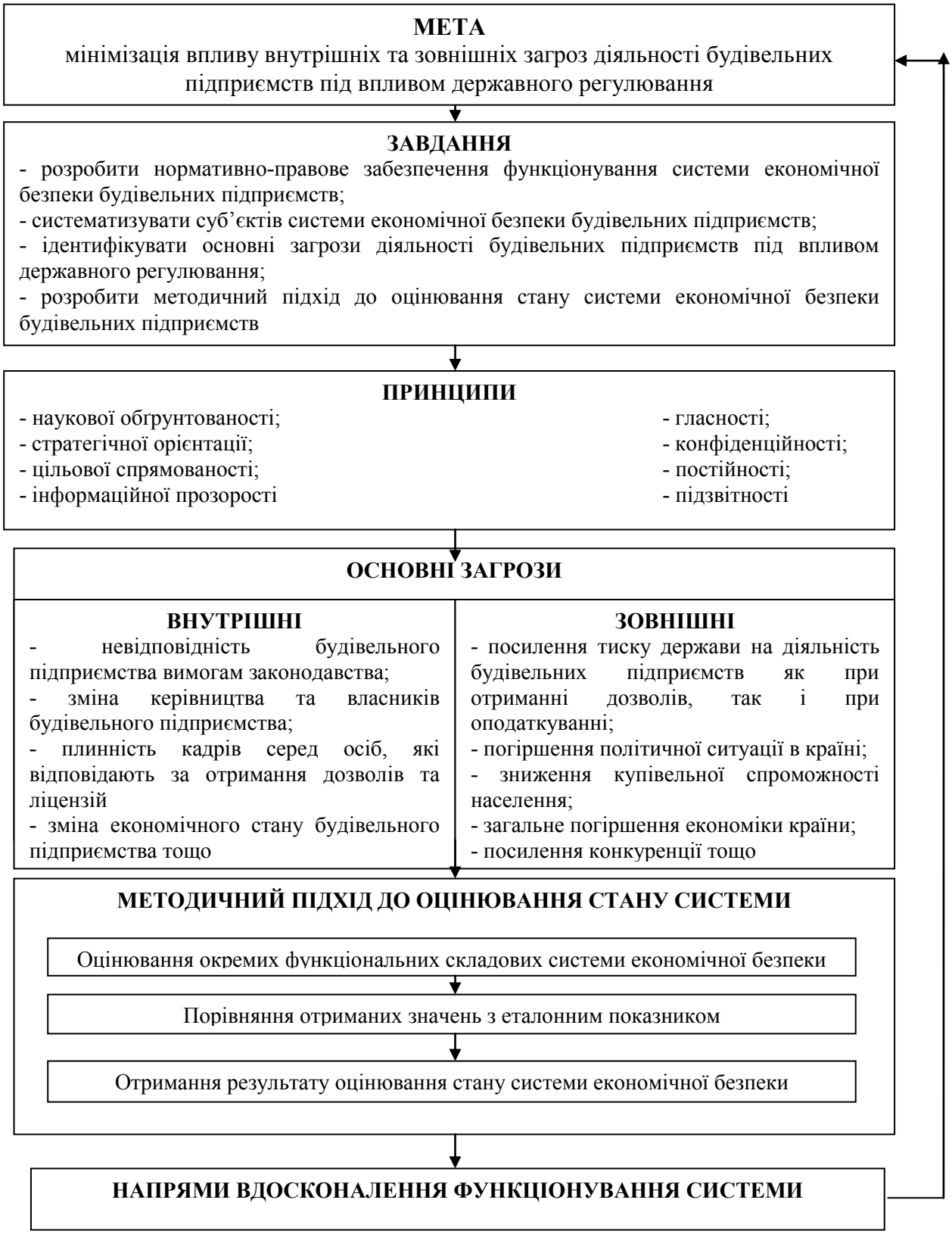


Рис. 2.5. Концепція вдосконалення системи економічної безпеки будівельного підприємства за умов впливу на неї державного регулювання

Створено автором

Наведені принципи дають основу для формування концепції вдосконалення системи економічної безпеки будівельних підприємств.

До концепції вдосконалення системи економічної безпеки будівельних підприємств обов'язково входять чинники, що впливають на функціонування такої системи.

Найважливішими внутрішніми загрозами функціонуванню системи економічної безпеки є:

- невідповідність будівельного підприємства вимогам законодавства;
- зміна керівництва та власників будівельного підприємства;
- плинність кадрів серед осіб, які відповідають за отримання дозволів та ліцензій;
- зміна економічного стану будівельного підприємства тощо.

Головними зовнішніми загрозами функціонуванню системи економічної безпеки є:

- посилення тиску держави на діяльність будівельних підприємств як при отриманні дозволів, так і при оподаткуванні;
- погіршення політичної ситуації в країні;
- зниження купівельної спроможності населення;
- загальне погіршення економіки країни;
- посилення конкуренції тощо.

Сукупність загроз, що здійснюють вплив на функціонування системи економічної безпеки пропонуємо розглянути шляхом поєднання складових механізму державного регулювання та функціональних складових системи економічної безпеки (табл. 2.1).

Таблиця 2.1

Матриця загроз функціонуванню системи економічної безпеки будівельних підприємств під впливом державного регулювання

		Складові механізму державного регулювання системи економічної безпеки будівельних підприємств			
		Економічний	Організаційно-управлінський	Технологічний	Соціальний
Функціональні складові системи економічної безпеки	Фінансова безпека	+		+	+
	Правова безпека	+	+		
	Кадрова безпека	+	+		+
	Технологічна безпека	+		+	
	Майнова безпека	+		+	
	Інформаційна безпека		+		
	Інтерфейсна безпека	+	+		+

Складено особисто автором

Таблиця 2.1 вказує на співвідношення між загрозами та складовими механізму державного регулювання системи економічної безпеки будівельних підприємств [3]. Отриманий результат вказує на те, що найсуттєвіший вплив на діяльність саме будівельних підприємств мають економічні та організаційно-управлінські важелі державного регулювання.

Саме тому створення та функціонування системи економічної безпеки вимагає розробки та реалізації механізму, який складається з:

а) організаційно-управлінського механізму функціонування системи економічної безпеки будівельних підприємств;

б) економічного механізму функціонування системи економічної безпеки будівельних підприємств.

Організаційно-управлінський механізм функціонування системи економічної безпеки включає:

а) методи, способи та прийоми організації системи економічної безпеки;

б) правове забезпечення організації системи економічної безпеки;

в) нормативне забезпечення організації системи економічної безпеки;

г) кадрове забезпечення організації системи економічної безпеки;

д) інформаційне забезпечення системи економічної безпеки.

Економічний механізм функціонування системи економічної безпеки включає:

а) методи та прийми впливу на економічний стан та економічне забезпечення господарської діяльності будівельних підприємств;

б) важелі впливу на економічний стан та економічне забезпечення господарської діяльності будівельних підприємств;

в) норми та нормативи економічної діяльності будівельних підприємств;

г) правове забезпечення економічної діяльності будівельних підприємств;

д) інформаційна база управління фінансами будівельних підприємств.

Механізми функціонування системи економічної безпеки в своїй сукупності впливають на вибір напрямів вдосконалення системи економічної безпеки будівельних підприємств, які залежать від економічної ситуації, а також від масштабів розвитку будівельних підприємств.

Запропонований концептуальний підхід до вдосконалення системи економічної безпеки може бути реалізовано для всіх груп будівельних підприємств. Це пов'язано як з масштабами економічно-господарської діяльності, так і з обсягами економічних втрат, які можуть зазнати будівельні підприємства. Найбільші втрати зазнають великі та крупні будівельні компанії, які мають значні обсяги економічно-господарської діяльності. Помітно менше економічних втрат зазнають середні будівельні підприємства. Невеликі будівельні підприємства у зв'язку з обмеженою економічно-господарською діяльністю мають найменші економічні втрати. Отже, концепція вдосконалення системи економічної безпеки розрахована перш за все на великі та середні будівельні компанії.

Для невеликих будівельних підприємств створення такої системи економічної безпеки може бути невигідно через значні витрати організаційного характеру.

Наукове значення запропонованого механізму функціонування системи економічної безпеки будівельного підприємства під випливом державного регулювання полягає у використанні теоретичних положень в діяльності суб'єктів будівельного бізнесу. Практичне значення полягає у можливості використання наукових розробок при створенні та функціонуванні системи економічної безпеки будівельних підприємств.

Для більшості середніх та невеликих будівельних підприємств запропонована механізм не може бути реалізований внаслідок необхідності створювати відповідні організаційні структури, залучати відповідних фахівців у сфері економічної безпеки, витрачати додаткові кошти на його створення та постійне функціонування.

Однак для великих та середніх будівельних підприємств такий механізм управління дає змогу суттєво підвищити ефективність системи економічної безпеки, своєчасно запобігати економічним загрозам і ризикам. Великі та середні будівельні підприємства значно виграють від реалізації такого механізму внаслідок того, що співвідношення між витратами на створення такого механізму і економічними втратами від різних економічних загроз і ризиків непорівнянні.

Забезпечення високого рівня економічної безпеки будівельних підприємств, можливо лише за умови постійного вдосконалення системи економічної безпеки в залежності від змін внутрішнього та зовнішнього середовища.

Головними результатами вдосконалення системи економічної безпеки будівельних підприємств під впливом державного регулювання повинно бути:

1) підвищення ефективності економічно-господарської діяльності будівельних підприємств;

2) зменшення економічних втрат від негативної дії загроз і ризиків;

3) зростання вартості будівельного підприємства;

4) задоволення інтересів власників будівельного підприємства;

5) задоволення інтересів трудового колективу будівельного підприємства;

6) виконання економічних вимог держави;

7) виконання економічних вимог кредиторів та партнерів по будівельному бізнесу.

Система економічної безпеки будівельного підприємства спрямована на забезпечення умов для підвищення ефективності економічно-господарської діяльності, зростання вартості підприємства, зменшення економічних втрат від реалізації різних загроз і ризиків. В кінцевому підсумку система економічної безпеки дозволяє забезпечити задоволення інтересів власників будівельних підприємств, керівництва та членів трудового колективу, виконання економічних вимог держави, виконання економічних вимог кредиторів і партнерів по будівельному бізнесу. [3]

Запропонований концептуальний підхід щодо вдосконалення системи економічної безпеки будівельних підприємств врівноважити стан зазначеної системи під впливом державного регулювання дозволить.

Список використаних джерел:

1. Андрієнко В. М. Безпека праці як складова системи економічної безпеки будівельних підприємств : монографія / В. М. Андрієнко. - Черкаси: Вид-во ТОВ «МАКЛАУТ», 2014. - 284 с.

2. Дмитренко В.І. Сучасні підходи до створення організаційно-економічного механізму управління діяльністю підприємств будівельної галузі / В. І. Дмитренко // Вісник Черкаського університету. Серія: економічні науки. – 2014. – №33 (326). – С. 38-42.

3. Дмитренко В.І. Вплив державного регулювання на систему економічної безпеки будівельних підприємств. Дис. канд. екон. наук: 21.04.02. – Режим доступу: https://drive.google.com/file/d/0Bz9Pblt6U8UmcWd1UEQxU3hicE0/view.

2.2. КОНЦЕПТУАЛЬНИЙ ПІДХІД ДО ВДОСКОНАЛЕННЯ ДЕРЖАВНОГО МОНІТОРИНГУ КОРУПЦІЙНИХ ЗАГРОЗ НА СИСТЕМУ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВНИМИ РЕГУЛЯТОРАМИ

ЧЕРЕВКО ОЛЕКСАНДР ВОЛОДИМИРОВИЧ, *д.е.н., професор,*
професор кафедри менеджменту та економічної безпеки,
ДМИТРОВА ОЛЬГА СЕРГІЇВНА*, здобувач*
кафедри менеджменту та економічної безпеки,
Черкаський національний університет імені Богдана Хмельницького

Національний банк України повинен ввести в дію методику оцінки рівня корупції у банківських установах, як частини захисту економічної безпеки банку. Згідно ст. 55 Закону України « Про Національний банк України» головна мета банківського регулювання визначається як безпека та фінансова стабільність банківської системи. Захист інтересів вкладників та кредиторів». Як вже було визначено, у попередніх розділах,система безпеки, повинна постійно змінюватись, щоб враховувати усі ризики. Не є винятком і НБУ. Його система нагляду, також повинна постійно змінюватись та оновлюватись.

Банківський нагляд - це система контролю та активних впорядкованих дій Національного банку України, спрямованих на забезпечення отримання банками та іншими особами, стосовно яких Національний банк України здійснює наглядову діяльність законодавства України і встановлених нормативів, з метою забезпечення стабільності банківської системи та захисту інтересів вкладників та кредиторів банку.

Метою праці банківського нагляду є підтримання стабільності банківської системи в межах свої повноважень та захист інтересів вкладників і кредиторів банку щодо безпеки зберігання коштів клієнтів на банківських рахунках.

Наглядова діяльність Національного банку України охоплює всі банки, їх відокремлені підрозділи, афілійованих та споріднених осіб банків на території України та за кордоном, установи іноземних банків в Україні, а також інших

юридичних та фізичних осіб у частині дотримання вимог Закону України "Про банки і банківську діяльність" щодо здійснення банківської діяльності.

На рисунку 2.6 зазначені основні метод державного та індикативного регулювання, які використовуються Національним банком України при роботі із комерційними банками.

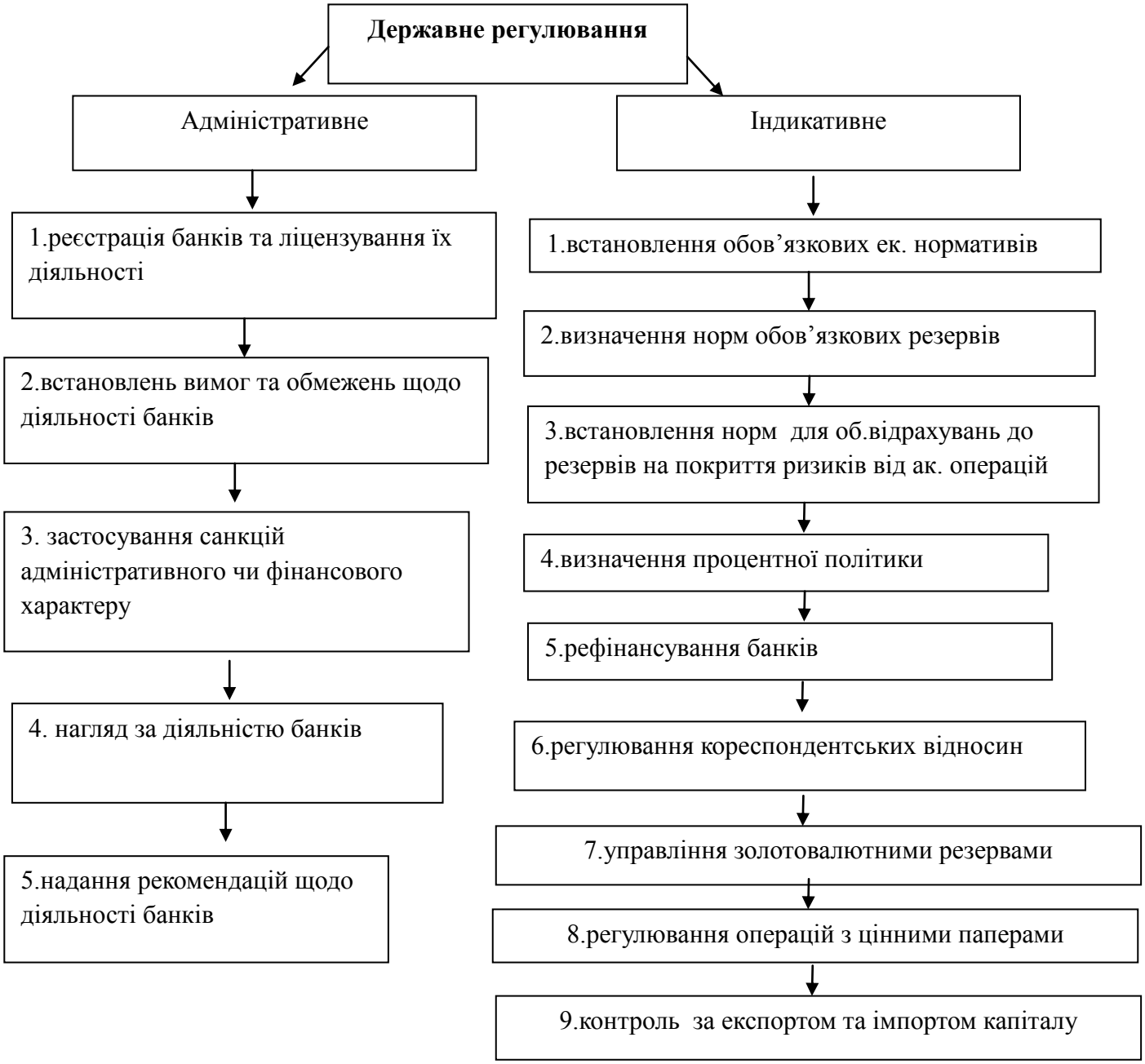


Рис. 2.6. Методи адміністративного та індикативного державного регулювання.

Для здійснення своїх функцій Національний банк України має право безоплатно одержувати від банків, банківських об'єднань та юридичних осіб, які отримали ліцензію Національного банку України, а також від осіб, стосовно яких Національний банк України здійснює наглядову діяльність відповідно до Закону України "Про банки і банківську діяльність", інформацію про їх діяльність та пояснення стосовно отриманої інформації і проведених операцій.

Як можна побачити з таблиці, основний напрям регулювання із сторони Національного банку України, спрямовано на впровадження за контролем виконання економічних нормативів у комерційному банку.

Але, на думку автора, одним із завдань Національного банку України, як контролюючого органу повинен стати контроль за рівнем корупції у банківському секторі .

Контроль за рівнем корупції у окремій банківській установі, потрібно розглядати як частину контролю за організацією системи ризик – менеджменту банку, яка впливає на економічну безпеку банку.

Якщо, система зовнішньої протидії економічній безпеці в першу чергу залежить від дій держави, та законодавчих актів. То побудова система внутрішньої економічної безпеці це завдання кожного окремого банку. Кожен банк повинен думати про мінімізацію своїх ризиків. Це необхідно для його виживання. НБУ повинен жорстко контролювати цей процес.

Головна відмінність запропонованого підходу полягає у тому, що автор пропонує здійснювати контроль не лише на рівні контролю за економічними нормативами банку, але й на рівні побудови системи управління банком.

Це має включати в себе:

- Контроль за організаційною структурою банку;
- Збільшення контролю за призначенням посадових осіб банку (не лише на рівні перевірки ділової репутації, але й на рівні визначення родинних зв'язків банку;
- Перевірку побудови системи економічної безпеку банку, в залежності від типу банку, напряму його діяльності, обсягу операцій, кількості філій тощо.

У таблиці 2.2. наведено етапи створення моделі забезпечення безпеки банківської установи.

Наведена модель являється уніфікованою, але при інспекційній перевірці банку, наглядові повинні враховувати наявність усіх вказаних етапів у банку.

Таблиця 2.2

Етапи створення моделі забезпечення безпеки банківської установи

№ п/п	Етап	Зміст етапу
1	Визначити цілі системи безпеки	Виділення пріоритетних видів безпеки
2	Виділити основні внутрішні та зовнішні загрози	Побудова карти внутрішніх і зовнішніх загроз
3	Розробити організаційно-правові основи побудови комплексної системи безпеки	Актуалізація законодавчого базису забезпечення безпеки освітнього закладу , розробка локальних актів ВНЗ, орієнтованих на вирішення основних завдань забезпечення безпеки
4	Забезпечити кадрами систему безпеки	Підбір кадрів, що володіють достатніми компетенціями в галузі забезпечення безпеки ВНЗ
5	Розробити технології, інструменти, методи та методики запобігання та протидії загрозам	Аналіз існуючих технологій, інструментів, методів і методик попередження, зниження рівня та протидії загрозам відбір і адаптація
6	Створити матеріально-технічне та фінансове забезпечення побудови та діяльності системи безпеки	Планування і виділення матеріально-технічних і фінансових ресурсів для забезпечення системи безпеки
7	Розробити механізми управління системою безпеки	Створення організаційної моделі управління системою безпеки як частини загальної організаційної структури ВНЗ
8	Організувати внутрішнє і зовнішнє взаємодія при здійсненні заходів щодо забезпечення безпеки та ін.	Розробка регламентів при проведенні заходів щодо забезпечення безпеки
9	Організувати моніторинг , аналіз і контроль за системою безпеки	Розробка регламентів з моніторингу, аналізу та контролю за системою забезпечення безпеки

**Складено автором*

Після підключення контролюючого органу, а саме Національного Банку України до оцінки рівня корупції у банківському секторі, потрібно вдосконалити методику оцінки рівня корупції у банківській установі.

Вдосконалення методики оцінки рівня корупції у банківській установі, потрібно починати з вдосконалення системи управління ризиками у банківській установі, а саме, запроваджувати роботу із корупційними ризиками у банківській установі, із самого початку – з моменту їх ідентифікації, до мінімізації самого виду ризику.

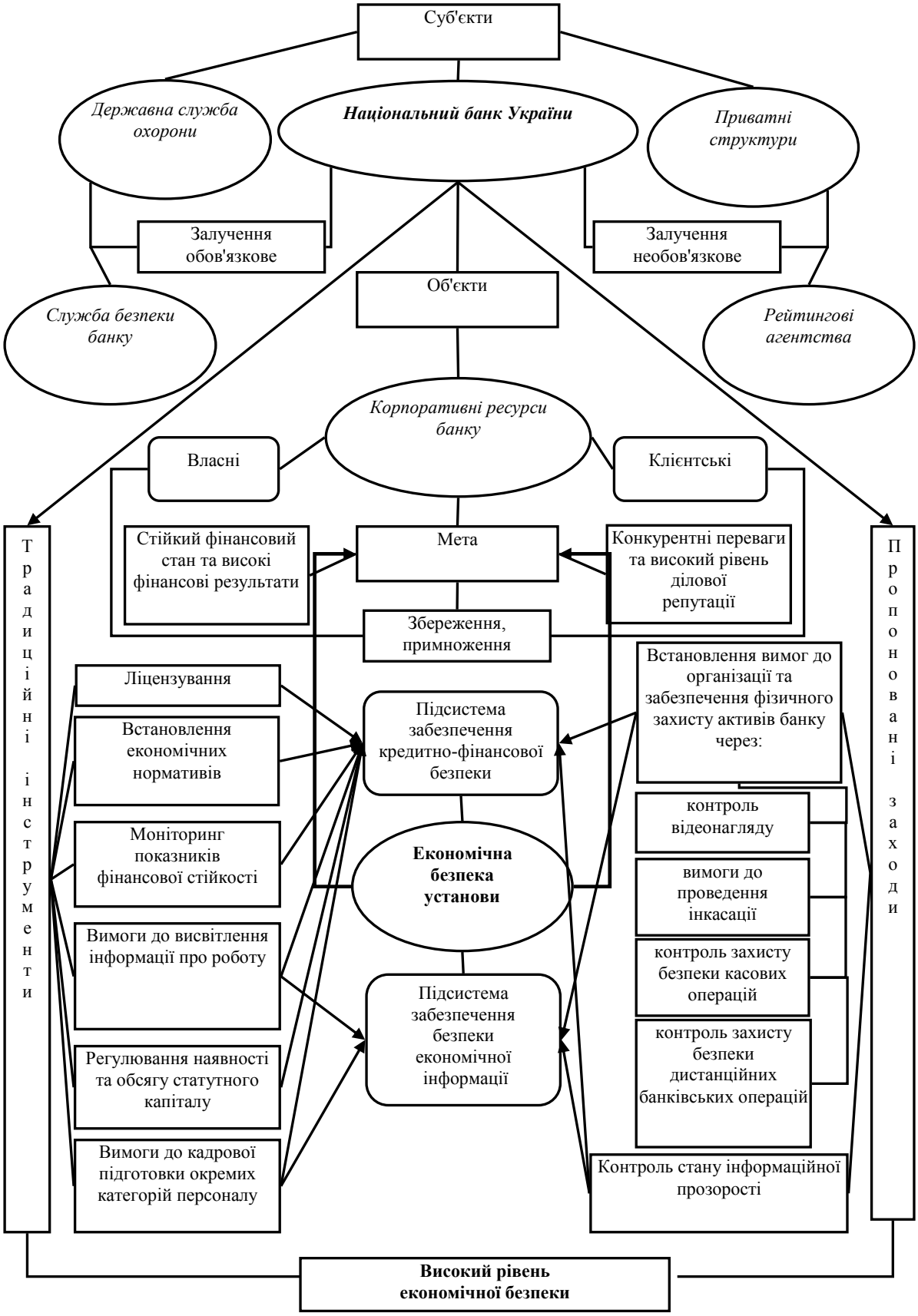


Рис. 2.7. Удосконалений механізм державного регулювання .

Мінімізація ризиків - це боротьба за зниження втрат. Цей процес містить у собі: передбачення ризиків, визначення їх імовірних розмірів та наслідків, розробку й реалізацію заходів щодо запобігання або мінімізації пов'язаних з ними втрат.

Мінімізувати ризики з урахуванням впливу зовнішнього середовища та специфіки діяльності банку має система управління ризиками, наявність якої є обов'язковою умовою успішної діяльності банківської установи. Наявність такої системи часто дозволяє уникати значних втрат. Усе це припускає розробку кожним банком власної стратегії керування ризиками, тобто основ політики прийняття рішень таким чином, щоб вчасно й послідовно використовувати всі можливості розвитку банку й одночасно втримувати ризики на прийнятному й керованому рівні.

Управління ризиками — одна з ключових функцій стратегічного управління банком із боку побудови системи економічної безпеки.Управління ризиками - це процедури і дії, які дозволяють менеджеру виявляти, оцінювати, відстежувати і усувати ризики до або під час їх перетворення у проблеми. Ризики бажано виявити якомога раніше і явно ще до того, як вони перетворилися на проблему (звичайно в цьому випадку прийняття заходів вимагає менших ресурсів). Після виявлення ризику необхідно прийняти рішення про відповідні дії. Завдання керівника банку - вибрати такі дії, які дозволять знизити ймовірність несприятливого події або зменшити його наслідки у разі реалізації ризику. При цьому бажано, щоб витрати ресурсів були мінімальними. Досягнути поставлених цілей можна шляхом створення комплексної системи управління ризиками. При побудові системи економічної безпеці – побудова ефективної системи управління ризиками це необхідна умова. І при цьому, система управління ризиками також оцінює ефективність управлінням економічною безпекою. З цією метою проводиться діагностичне обстеження, котре включає в себе аналіз та оцінку фінансового стану і тенденцій розвитку банку, а також виявлення позитивних чи негативних чинників впливу на його фінансову стійкість .

Ефективність діагностичного обстеження вища тоді, коли визначено такі етапи її проведення: встановлення належності об'єкта до певного класу або групи об'єктів; виявлення відмінностей об'єкта, що діагностується, від об'єктів свого класу шляхом порівняння його фактичних параметрів із базовими; розробка та реалізації адекватних антикризових заходів. Якість оцінки економічної безпеки залежить від глибини, повноти обліку всіх факторів, що визначаються станом інформаційного забезпечення. Тобто, чим більше факторів у нас є для аналізу, тим більш вірною буде оцінка та визначення пріоритетних ризиків для банку. І керівництво ризику зможе визначити прийняття чи не прийняття будь якого виду ризику, але при цьому,враховуючи багатогранність поняття економічної безпеки банку, можливо зробити висновок, що кожен з даних видів ризику, впливає на економічну безпеку банку. – або кожен з перелічених видів ризику несе в собі ймовірність збитку для банку, а значить впливає на економічну безпеку банку.

При цьому, етапи створення організаційно – функціональної системи управління корупційними ризиками як частини економічної безпеки є наступними:

1. Етап виявлення джерел (видів) ризику на процесах:

- декомпозиція кожного процесу банку на складові його операції;
- складання технологічної карти документообігу процесу;
- збір даних про несприятливі події та втрати;
- ідентифікація на кожній операції можливих проявів окремих джерел (видів) ризику.

На рис. 2.8 Наведено приклад технологічної карти бізнес - процесу надання кредитів.

Така декомпозиція кожного процесу банку на складові його операції дозволяє виявити всередині банку, на якому етапі можливо проявлення корупційного ризику. Ідентифікація корупційного ризику повинна охоплювати всі напрямки діяльності Банку з метою визначення існування або можливості виникнення подій КР в банківських процесах, продуктах, системах.

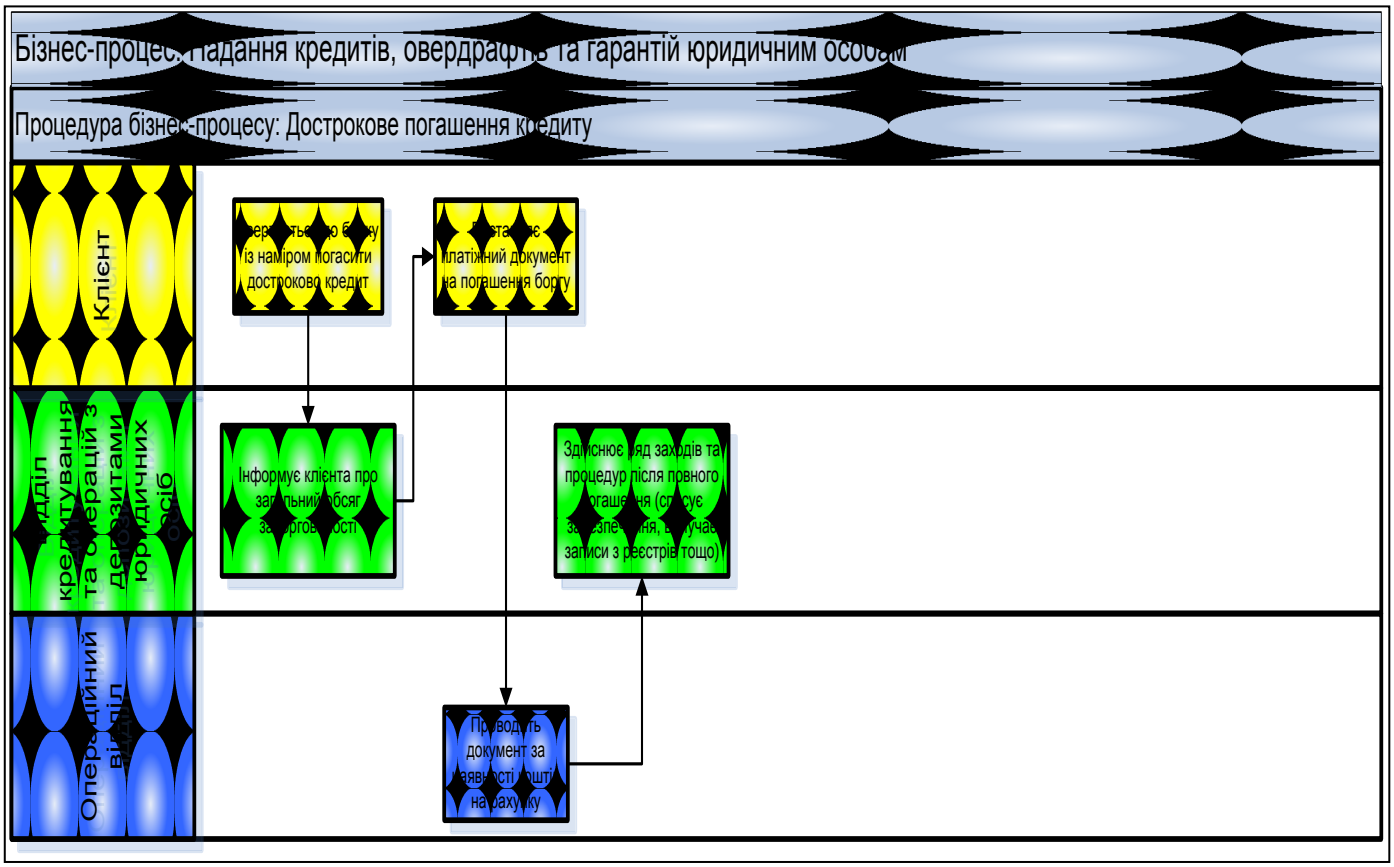


Рис. 2.8.Технологічна карти процесу надання кредитів. Процедура погашення кредиту

**складено автором*

Дана робота повинна проводитись на етапі розробки і затвердження нових банківських продуктів, процесів, систем підрозділами Банку повинен бути проведений відповідний аналіз з метою визначення подій реалізації корупційного ризику, характерних нововведенню, а також адекватних заходів, направлених на мінімізацію і контроль рівня корупційного ризику.

2. Етап є створення організаційної системи виявлення, вимірювання і управління корупційними ризиками.

Бажано, щоб питаннями виявлення, вимірювання і управління корупційними ризиками займався один підрозділ, але враховуючи той факт, що банківським установам економічно не вигідно збільшувати штат працівників, які не приносять явного та прямого прибутку, у якості підрозділу по роботі з

корупційними ризиками може виступати як банківська безпека так і підрозділ по роботі з операційними ризиками.

Даний підрозділ на регулярній основі формує звітність, що відображає загальну величину та структуру корупційних ризиків Банку для прийняття управлінських рішень з управління корупційних ризиків з урахуванням інших ризиків, наявних у Банку.

З метою виявлення індивідуальних ризиків проводиться анкетування структурних підрозділів банку у термін не частіше ніж раз на рік. На основі анкетування та інших даних складається каталог корупційних ризиків банку. Форма анкети може бути якою завгодно. Найголовніше – вона повинна включати в себе наступні питання:

- Де саме виникає корупційний ризик?
- Як часто?
- Хто фіксує ці інциденти?
- Які фінансові втрати завдає той чи інший тип (вид) корупційного ризику?

Моніторинг за частотою та проявом інцидентів корупційного ризику – дозволяє здійснювати поточний контроль, спостереження, нагляд за корупційними ризиками, подіями, пов’язаними з їх реалізацією безпосередньо в ході операційної роботи. Моніторинг передбачає постійне, систематичне і послідовне відстеження та попередження корупційних ризиків.

Моніторинг корупційного ризику проводиться як на рівні структурних підрозділів, так і в цілому по банку.

Поточний моніторинг ризиків – це внутрішній оперативний поточний контроль та ризиками, які властиві напряму діяльності підрозділу, що здійснює операційний моніторинг. Постійний моніторинг сприяє оперативному виявленню та вжиттю заходів щодо мінімізації наслідків корупційного ризиків

Звіти про величину корупційних ризиків, включаючи інформацію про пов'язані з ними фінансові втрати, повинні на регулярній основі надаватися керівникам структурних підрозділів, Правлінню Банку.

3. Етап створення методології та технології вимірювання корупційних ризиків складається із декількох етапів.

Перший це – моніторинг та контроль корупційного ризику.

Моніторинг і контроль рівня корупційного ризику здійснюється через:

- обговорення і оцінку звітів з корупційного ризику (звіти про втрати, звіти про КПР, результати самостійної оцінки корупційних ризиків та заходів контролю, результати сценарного аналізу);
- обговорення і оцінку звітів внутрішньої і зовнішніх служб аудиту,
- відслідковування прогресу у виконанні відповідальними підрозділами Банку рекомендацій служб аудиту, органів нагляду,
- розвиток і відслідковування досвіду, отриманого із внутрішніх (і зовнішніх по відношенню до Банку) подій КР,
- обговорення і оцінку методів розрахунку резервного капіталу під КР – відповідно оцінку результатів розрахунку,
- прийняття відповідних управлінських рішень.

Другий етап – це процес розробки та впровадження виправних заходів по подіях КР

Підрозділ, відповідальний за подію КР, складає план виправних заходів за подією КР із зазначенням термінів виконання, відповідальних за виконання підрозділів / осіб за кожним заходом. План виправних заходів за подією КР також надається Підрозділу по роботі з операційними ризиками у складі повідомлення про подію КР згідно з окремим внутрішнім нормативним документом Банку, що регламентує порядок збору інформації про події реалізації корупційного ризику.

Збір та аналіз зовнішніх даних про втрати в банківській сфері внаслідок реалізації подій КР є джерелом даних для наступного аналізу з метою визначення стратегії поведінки Банку при реалізації конкретної події ОКР, суми потенційних втрат, тощо. З цією метою Банк відслідковує зовнішні по відношенню до Банку події КР та проводить аналіз вразливості Банку до

відповідних подій (ризиків) шляхом аналізу таких джерел інформації про зовнішні події:

- Засоби масової інформації;
- Зовнішні бази даних подій корупційного ризику, як знаходяться в загальному доступі;
- Конференції, семінари, зустрічі представників банківського сектору і т.д.

Самостійна оцінка корупційних ризиків та заходів контролю (далі – СКРК) – інструмент, який використовується підрозділами Банку для ідентифікації подій корупційного ризику (ризиків), притаманних процесу, продукту, системі, що аналізується; визначення вад системи внутрішнього контролю в операціях, які виконуються щоденно з метою визначення/розробки заходів, направлених на попередження/мінімізацію подій корупційного ризику.

СКРК є безперервним процесом, метою якого є гарантування, що усі події корупційного ризику (ризики) виявлені, інформація по ним доведена до топ-менеджменту Банку і по їх управлінню прийняте рішення особою, що має такі повноваження.

В рамках СКРК може застосовуватися метод оціночних карт (score-cards), що має на меті визначення найбільш істотних факторів (причин) корупційного ризику, пов'язаних з поточними умовами діяльності Банку, а також дозволяє здійснювати моніторинг зміни рівня корупційного ризику за різними процесами, в т.ч. супроводжуючими.

Метод припускає заповнення підрозділами Банку централізовано розробленихх підрозділом по роботі з корупційними ризиками опитувальних анкет-карток, що містять орієнтовно до 30 питань з якісної оцінки рівня ризику.

Перелік питань покриває аспекти ймовірності та істотності фактичних і потенційних подій КР, рівня застосовуваного внутрішнього контролю, а також можливих мір, спрямованих на зниження ймовірності подій КР і величини потенційних втрат. Ризики ідентифікуються (виявляються) і оцінюються на підставі єдиної класифікації корупційних ризиків (подій КР) згідно з відповідним внутрішнім нормативним документом Банку, який визначає

порядок збору інформації про події реалізації корупційного ризику. Отримані агреговані результати аналізуються на предмет виявлення в процесах (в т.ч. супроводжуючих) «слабких» зон, найбільш схильних до корупційного ризику, з наступним вжиттям заходів щодо їх усунення.

Процедура СКРК курується (координується) та контролюється Підрозділом по роботі з корупційними ризиками. Структурні підрозділи Банку повинні формувати звіти по СКРК та надавати їх в Підрозділ по роботі з корупційними ризиками. Після обробки, звіти (узагальнені) за найбільш критичними КР (за ймовірністю настання та величиною втрат (в т.ч. неприйнятних)) повинні виноситися на розгляд Правлінню Банку.

Правила та детальний порядок проведення СКРК, в тому числі форми звітів, підлягають визначенню відповідним окремим внутрішнім нормативним документом Банку.

Ключові показники ризику (КПР) використовуються для відстеження і прогнозування тенденцій зміни рівня корупційного ризику. Регулярний моніторинг КПР дозволяє здійснювати аналіз небажаних подій корупційного ризику і розробляти попереджуючі заходи, направлені на мінімізацію ймовірності її реалізації.

З метою аналітичної роботи під час оцінки корупційного ризику КПР можуть бути умовно (за змістом) розподілені на такі види:

– *показники діяльності* – максимально припустиме число окремих найбільш важливих для Банку подій КР, що відбулися за встановлений період часу, при перевищенні якого варто вживати заходів щодо нейтралізації корупційного ризику. Частота проведення моніторингу індикаторів діяльності може різнитися залежно від їхнього ступеня впливу на результати діяльності Банку;

– *показники ефективності контролю* – показники, що характеризують якість і ефективність існуючих у Банку механізмів внутрішнього контролю. Такими показниками можуть бути, у т.ч., число виявлених порушень співробітниками встановлених посадових обов'язків і повноважень, фальшивих

банкнот, підроблених чеків, число неврегульованих позицій або сторнованих записів за рахунками бухгалтерського обліку, непідтверджених контрагентами операцій тощо;

– *комплексні ключові показники ризику* – найбільш важливі комбінації окремих *показників діяльності* і *ефективності контролю*, моніторинг яких повинен здійснюватися Банком найчастіше.

- Мінімальний набір КПР, які відстежуються в Банку включає в себе:
- Кількість скарг від клієнтів, партнерів;
- Кількість критичних збоїв системи та час простою;
- Кількість помилок, виявлених Службою внутрішнього аудиту;
- Кількість позовних справ;
- Плинність кадрів.

Форми та перелік звітів по КПР (в т.ч. перелік відповідальних підрозділів Банку) затверджуються рішенням Правління Банку, після чого із визначеною Правлінням Банку періодичністю (або за запитом Підрозділу по роботі з корупційним ризиком – у разі обґрунтованої необхідності) надаються відповідними підрозділами Банку до Підрозділу по роботі з корупційними ризиками.

Можливими джерелами даних про події КР для їх аналізу та оцінки величини втрат, а також перевірки повноти та якості інформації в базі даних про події КР є:

- відомості структурних підрозділів про фактичні і/або потенційні події КР (в т.ч. втрати внаслідок подій КР), обумовлені проведенням операцій;
- відомості бухгалтерського обліку про втрати Банку, пов'язані з виявленими подіями КР;
- акти перевірок діяльності підрозділів Банку;
- інформація про судові спори;
- результати службових перевірок та службових розслідувань;
- перелік скарг клієнтів/співробітників щодо якості надання продуктів/послуг;

•інформація про несанкціоновані операції з платіжними картками клієнтів, які призвели до втрат Банку;

тощо.

Усі втрати Банку внаслідок реалізації подій КР збираються у окрему аналітичну базу даних подій КР. Детальна класифікація подій корупційного ризику є основою для подальшого аналізу корупційних втрат, а також для формування регулярної звітності для керівництва Банку.

Підрозділ по роботі з корупційними ризиками консолідує надані підрозділами звіти, проводить аналіз, моніторинг та контроль діяльності підрозділів Банку:

•відстежує в часі значення КПР і відповідний рівень корупційного ризику;

•у разі потреби – для певних КПР встановлює певний ліміт, який не повинен перевищуватись;

•визначає необхідні засоби уникнення/мінімізації ризиків та сприяє їх впровадженню.

Результати аналізу надаються у складі звітності по корупційним ризикам на розгляд Правлінню Банку для прийняття відповідних управлінських рішень.

4. Створення методологічних основ прийняття ризику або розробка інструментів імунізації та заходів зниження ризику на окремих процесах або операціях.

Організаційно це завдання вирішується шляхом створення спеціального допоміжного підрозділу з оцінки та контролю за ризиками, (або добавлянням окремої функції в уже існуючий підрозділ по роботі з операційними ризиками) в основні функції якого можуть входити:

•розробка політики з управління ризиками на підприємстві, включаючи вимоги до звітності для керівників функціональних підрозділів і вищого керівництва;

•координація щоденного процесу управління ризиками;

•оцінка сукупних ризиків компанії на основі єдиного і послідовного підходу і відстеження фінансових ринків і інших подій в економічному житті, які можуть вплинути на розмір прийнятих ризиків;

•розробка, тестування і санкціонування застосування методів і моделей оцінки ризиків, особливо що використовуються для ціноутворення фінансових інструментів і продуктів;

•створення і ведення баз даних, необхідних для цілей ризик-менеджменту;

•взаємодія зі службами внутрішнього контролю з метою забезпечення дотримання вимог законодавства, регулюючих органів, а також внутрішніх положень та процедур;

•доведення результатів оцінки та управління ризиками до керівництва банку, а також підготовка інформації для регулюючих органів, інвесторів і рейтингових агентств.

5. Зниження, уникнення, запобігання корупційному ризику.

Банк може прийняти такі рішення щодо виявлених ризиків:

•Прийняття ризику(усвідомлення та прийняття певної порції ризику, як природної, невід'ємної в процесі прийняття рішень, тобто визначення рівня прийнятності ризику);

•Зменшення імовірності реалізації ризику (вдосконалення процесу, продукту, системи (в т.ч. впровадження контролю процесів, проведення тестування, тренінгів);

•Запобігання/уникнення ризику (може досягатись за допомогою припинення того виду діяльності, який генерує ризик (в т.ч. відмова чи обмеження надання продукту чи послуги), передачі такої діяльності на виконання сторонніми організаціями (аутсорсинг), ін.).

•Зменшення наслідків від реалізації ризику (страхування певного виду корупційного ризику, впровадження виправних заходів за подіями КР).

6. Зменшення імовірності реалізації корупційного ризику.

Зменшення імовірності реалізації корупційного ризику здійснюється наступним чином:

•Розробка і реалізація заходів, направлених на обмеження та нейтралізацію виявлених критичних зон ризику в системах, продуктах/послугах, процесах (в т.ч. впровадження контрольних заходів);

•Розвиток і вдосконалення банківських технологій (в т.ч. автоматизації процесів), правил і процедур здійснення операцій;

•Стандартизація банківських продуктів/послуг, процесів;

•Забезпечення співробітників Банку максимально повними, адекватними, чіткими та зрозумілими внутрішніми нормативними документами;

•Побудова і підтримка ефективної системи захисту інформації;

•Розвиток мотивації співробітників, їх навчання і підвищення кваліфікації;

•Підвищення ефективної системи внутрішнього контролю;

•Підвищення ефективної організаційної структури.

Також, із сторони контролюючих органів необхідно законодавчо закріпити. Що основними складовими системи запобігання корупції в приватному секторі у тому числі і банківському є і повинно бути:

•юридичні особи розробляють та реалізують антикорупційні заходи;

•керівництво або засновники чи учасники зобов'язані здійснювати періодичну оцінку корупційних ризиків та здійснювати антикорупційних заходів – для виявлення ризиків можливо залучати незалежних експертів, в тому числі для проведення аудиту ;

•працівники юридичних осіб зобов'язані дотримуватися стандартів доброчесності;

•юридичні особи розробляють внутрішні антикорупційні програми, які передбачають комплекс заходів із запобігання корупції (правила запобігання корупції, процедури їх дотримання та моніторингу, правила етичної поведінки, механізми захисту інформаторів, інформування про конфлікт інтересів правила його врегулювання, порядок консультування працівників тощо) – стосується лише двох категорій компаній - державних, комунальних підприємств, господарських товариств (у яких державна або комунальна частка перевищує 50 відсотків), де середньооблікова чисельність працюючих за звітний (фінансовий)

рік перевищує п’ятдесят осіб, а обсяг валового доходу від реалізації продукції (робіт, послуг) за цей період перевищує сімдесят мільйонів гривень; юридичних осіб, які є учасниками попередньої кваліфікації, учасниками процедури закупівлі відповідно до Закону України «Про здійснення державних закупівель», якщо вартість закупівлі товару (товарів), послуги (послуг) дорівнює або перевищує 1 мільйон гривень, а робіт - 5 мільйонів гривень;

•керівник юридичної особи, де затверджується програма, визначає уповноважену особу з антикорупційних питань, яка відповідає за реалізацію програми (Законом встановлюються вимоги до уповноважених осіб, визначається спеціальний перелік підстав для звільнення уповноваженої особи).

Ці правила безпосередньо пов‘язані з відповідальністю юридичних осіб - незабезпечення виконання покладених на уповноважену особу законом або установчими документами юридичної особи обов’язків щодо вжиття заходів із запобігання корупції, якщо це призвело до вчинення корупційного злочину, є самостійною підставою для застосування до юридичної особи заходів кримінально-правового характеру.

Наразі досить важливим завданням як для влади, так і для бізнесу та громадськості – це пропагування впровадження зазначених правил серед компаній.

Список використаних джерел:

1. *Крупка І. М. Фінансово-економічна безпека банківської системи України та перспективи розвитку національної економіки / І. М. Крупка // Бізнес-Інформ. — 2012. — № 6. — С. 168–175.*
2. *Васильчак С. В. Економічна безпека банків та методи її забезпечення / С. В. Васильчак, Р. Ю. Моцьо // Науковий вісник НЛТУ України. — 2009. — № 19.12. — С. 287–293.*
3. *Дудченко Н. В. Необхідність забезпечення економічної без пеки на всіх рівнях / Н. В. Дудченко //Безпекознавство: теорія та практика : матеріали І Всеукр. наук.-практ. Інтернет-конф., 15 берез.–15 квітн. 2013 р. – Луганськ: СНУ ім. В. Даля, 2013. — С. 60–62.*
4. *Дудченко Н.В. Вплив державного регулювання на систему економічної безпеки банківських установ // Дисертація на здобуття наукового ступеня кандидата економічних наук. УДК 336.761 - Черкассы 2015.*
5. *Дудченко Н. В. Система економічної безпеки комерційних банків України: сутність та структура / Н. В. Дудченко // Банківська система України в умовах глобалізації фінансових ринків : VII Міжнар. наук.-практ. конф., 18–19 жовт. 2012 р. : тези доповід. — Черкаси: ЧІПС УБС НБУ, 2012. — С. 87–89.*
6. *Дмитрова О.С. Класифікація загроз та ризиків економічної безпеки банків [Електронний ресурс]. - Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=4599*

7. Дмитрова О.С. Загрози економічної безпеки, як складова системи ризик-менеджменту банку [Електронний ресурс]. - Режим доступу: file:///C:/Users/HOME_PC/Downloads/243-443-2-PB.pdf.
8. Стельмах В.С. та ін. Контроль: інспектування, аудит, банківський нагляд: Монографія / В.С. Стельмах, А.О. Єпіфанов, І.В. Сало, М.А. Єпіфанова. - Суми: ВТД "Університетська книга", 2006. - 432 с.

2.3. МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ СЛУЖБАМИ БЕЗПЕКИ ОХОРОННИХ ПІДПРИЄМСТВ

***МІНЕНКО МАРГАРИТА ВІКТОРІВНА**, к.е.н.*
***МІГУС ІРИНА ПЕТРІВНА,** д.е.н., професор,*
завідувач кафедри менеджменту та економічної безпеки,
Черкаський національний університет імені Богдана Хмельницького

Для забезпечення економічної безпеки підприємствам не обійтись без використання послуг відповідних фахівців. Необхідність таких послуг зумовлена сильною конкурентною боротьбою на зовнішньому та внутрішньому ринках, а також нерідкими проявами промислового шпіонажу. Завдяки залученню служб безпеки суттєво знижується комерційний ризик та підвищується рівень безпеки підприємницької діяльності.

Велика кількість загроз економічній безпеці підприємств спонукала розробку основних напрямків їх усунення. Головний з них – розробка механізму, що міг би забезпечити стійку економічну безпеку суб’єктів господарювання. Особливість системи економічної безпеки господарської діяльності полягає в тому, що захист підприємства відбувається враховуючи всі напрями та сфери його діяльності. Одним з найефективніших інструментів підвищення рівня економічної безпеки суб’єктів господарювання повинен стати механізм його забезпечення, що має об’єднувати в собі сукупність законодавчих актів, правових норм, спонукальних мотивів та стимулів, методів, засобів та заходів, які необхідні для досягнення поставлених цілей безпеки та розв’язання поставлених задач.

Пропонуємо під поняттям «механізм забезпечення економічної безпеки службами безпеки охоронних підприємств» розуміти сукупність методів і заходів щодо практичного забезпечення безпеки суб'єктів господарювання охоронними підприємствами.

Механізм забезпечення економічної безпеки підприємств, що виконується охоронними організаціями, повинен реалізовуватись, як певний комплекс

заходів в інтересах суб’єктів господарювання від внутрішніх та зовнішніх негативних ризиків. Основна мета механізму – створення оптимальних умов для надання захисту кожному суб’єкту, що входять в систему корпоративної відповідальності охоронної форми. При цьому сама охоронна організація виступає в якості гаранта захисту та реалізації основних потреб безпеки. Завдяки роботі чітко злагодженого механізму з ефективним використанням всіх методів і засобів забезпечується стабільність діяльності підприємства, створюються нові умови для сталого розвитку.

Відповідно до мети дослідження та функціональних складових економічної безпеки, механізм повинен вирішувати ряд завдань, наведених в таблиці 2.3 [6].

Таблиця 2.3

Завдання механізму забезпечення економічної безпеки

Складові економічної безпеки	Завдання механізму забезпечення економічної безпеки
Фінансова	аудит з точки зору економічної безпеки підприємства, пошук та аналіз слабких місць з метою поліпшення показників
	моніторинг, прогнозування та своєчасне виявлення причин та умов, що ведуть до фінансових збитків підприємства
	створення механізму та умов оперативного реагування щодо випадків шахрайства, що спостерігається з боку співробітників підприємства
	формування системи обліку фінансових потоків
Кадрова	ефективне усунення будь-яких загроз працівникам суб'єкта господарювання
	створення спеціальної системи підготовки, перепідготовки та підвищення кваліфікації персоналу суб'єктів безпеки
	організація та супровід кадрової роботи (з позиції захисту економічної безпеки підприємства)
	аналіз роботи всіх співробітників
Силова	фізична охорона об’єктів, території, процесів та персоналу
	розробка і впровадження режимних заходів, головною задачею яких є виключення або ускладнення спроб завдати збитку підприємству, включаючи нанесення фізичної шкоди
	проведення внутрішніх розслідувань подій на підприємстві і в зоні його інтересів
	присутність на різних заходах підприємства (виставки, презентації, переговори, зв’язки із громадськістю, PR-компанії тощо)
Пожежна	моніторинг, аналіз та прогнозування, вчасне виявлення та усунення загроз пожежній безпеці суб'єкта господарювання
	проведення контролю за дотриманням вимог пожежної безпеки персоналом
	регулярна перевірка обладнання, що необхідне для пожежного захисту

Складові економічної безпеки	Завдання механізму забезпечення економічної безпеки
	послаблення негативного впливу наслідків від порушень правил пожежної безпеки
Інформаційна	збір необхідної інформації. При цьому можуть використовуватись технічні засоби на підприємстві та поза його межами
	аналіз, оцінка інформації, виявлення певних тенденцій, прогнози та вироблення рекомендацій стратегічного характеру на основі існуючих даних
	створення єдиної інформаційної бази даних
	забезпечення заходів по захисту конфіденційності інформації, яка є комерційною таємницею
Екологічна	розробка та впровадження заходів, що стосуються енергозбереження та екологічної безпеки на підприємстві
	вивчення, аналіз та впровадження заходів для підвищення рівня в сфері екологічної безпеки
	аналіз власних зон вразливості та здійснення заходів для їх елімінації, маскування або захисту
	визначення нових, більш перспективних напрямів діяльності і вдосконалення роботи щодо створення найбільш сприятливих екологічних умов для безпечного функціонування підприємства
Технологічна	ведення боротьби за ринок та ресурси із застосуванням методів, які не входять в рамки традиційного маркетингу
	вивчення контрагентів
	вивчення конкурентів, їх поточного стану справ та перспектив розвитку, планів, можливостей, кадрів, ресурсів, новинок, виявлення їх сильних та слабких сторін
	постійний контроль внутрішніх та зовнішніх процесів на підприємстві, що необхідно для недопущення небезпечного розвитку подій
Майнова	усунення будь-яких загроз, посягань на ресурси суб'єкта господарювання завдяки застосуванню правових, організаційних та інженерно–технічних заходів і засобів досягнення необхідного рівня безпеки підприємства
	створення нормативно-правового механізму для максимально можливої локалізації та відшкодування спричинених збитків, що були нанесені в результаті неправомірних дій фізичних чи юридичних осіб
	своєчасне виявлення та аналіз реальних і потенціальних загроз майну підприємства. Це стосується як внутрішнього, так і зовнішнього середовища
	створення ефективного механізму взаємодії між державними структурами та суб’єктами господарювання в питаннях безпеки

Складено автором

Для ефективного забезпечення економічної безпеки охоронні підприємства мають виконувати завдання служб безпеки відповідно до функціональних складових [1].

Відповідно до функціональних складових економічної безпеки виділено перелік функцій та інструментів для систематизації та оперативного прийняття відповідних мір (рис. 2.9).

Рис. 2.9. Функції та інструменти механізму забезпечення економічної безпеки

Складено автором

Механізм забезпечення безпеки служб безпеки охоронними підприємствами будується на принципах, описаних на рисунку 2.10.

Не менш відомим фактом є роль забезпеченості підприємства усіма необхідними видами ресурсів, так зване ресурсне забезпечення

підприємницької діяльності: інформаційні, фінансові, правові, трудові, нематеріальні, матеріальні, технологічні ресурси.

Принцип законності	• Система безпеки будується і здійснюється виключно у правовому полі на основі норм українського законодавства із застосуванням дозволених законодавством України форм, методів, засобів, технік і технологій забезпечення безпеки.
Принцип економічної доцільності	• Всі витрати на створення системи безпеки повинні окупатися прибутком, отриманим суб'єктами господарювання в результаті здійснення заходів з протидії загрозам, викликам і небезпекам. Витрати на створення системи безпеки не повинні призводити до погіршення економічних показників діяльності.
Принцип комплексності	• Вся діяльність з протидії загрозам, викликам і небезпекам повинна здійснюватися на основі розробленої політики і стратегії безпеки, із залученням усіх наявних в фінансових, матеріально-технічних, інтелектуальних, інформаційних та інших ресурсів
Принцип безперервності	• Діяльність із забезпечення безпеки носить безперервний характер. Це обумовлено тим, що в умовах ринкової економіки небезпеки, загрози і ризики носять перманентний характер.
Принцип взаємодії та координації	• Забезпечення безпеки має здійснюватися на основі тісної взаємодії та координації діяльності служби безпеки охоронного підприємства зі штатними підрозділами безпеки суб'єкта господарювання, іншими структурними підрозділами.
Принцип закритості та гласності	• Система безпеки повинна працювати гласно. Керівники, а також персонал повинні постійно інформуватися фахівцями безпеки про загрози та ризики і отримувати рекомендації з протидії їм. В окремих випадках діяльність щодо забезпечення безпеки може носити закритий характер. Сама специфіка забезпечення безпеки вимагає від її суб'єктів не поширювати наявну у них інформацію про форми і методи забезпечення безпеки.

Рис. 2.10. Принципи дії механізму забезпечення економічної безпеки суб’єктів господарювання

Необхідним є безперервний циклічний процес пошуку, залучення та використання різних видів ресурсів, необхідних для запобігання можливих зовнішніх та внутрішніх загроз та/або різнобічного взаємоузгодження

економічних інтересів підприємства. Ресурсне забезпечення економічної безпеки підприємства вимагає значних витрат і ґрунтується на комплексному використанні всіх ресурсів, їх відповідності за якістю і кількості і здатності керівництва використовувати традиційні види ресурсів в новому призначенні

Відповідно, чим вищим є ресурсне забезпечення підприємства та служб безпеки, тим вищим є і сам рівень економічної захищеності організації.

Автором сформована «Матриця управлінських рішень з попередження загроз економічній безпеці» (табл. 2.4), в основу якої покладені принципи прийняття управлінських рішень. Матриця є комплексом взаємопов'язаних елементів всередині багаторівневої структури, що взаємодіють для забезпечення економічної безпеки суб'єктів господарювання. І заходяться під постійним впливом зовнішніх і внутрішніх загроз [2].

В основу механізму вирішення завдань економічної безпеки суб'єктів господарювання покладений принцип субсидіарності, який полягає у тому, що попередження загроз економічній безпеці повинно виконуватись на мікроекономічному рівні.

Для практичного втілення виділено шість рівнів в процесі діяльності суб'єктів господарювання: перший рівень – власники, засновники, акціонери; другий рівень – топ-менеджмент, дирекція; третій рівень – персонал; четвертий рівень – організація бізнес-процесів; п'ятий рівень – поточна діяльність; шостий рівень – облік, аналіз, аудит.

Практична реалізація механізму вирішення завдань економічної безпеки службами безпеки охоронних підприємств здійснюється використанням матриці співвідношення загроз економічній безпеці, згрупованих за функціональними складовими та шести рівнів управління суб'єктів господарської діяльності.

Правило прийняття рішення означає, що чим лівіше розміщений стовпчик і вище – рядок, тим вище важливість і результативність управлінського рішення протидії загрозам економічної безпеки.

Таблиця 2.4

Матриця управлінських рішень щодо попередження загроз економічній безпеці суб'єктів господарювання

Рівні управління / Функціональні складові системи економічній безпеці	**1 рівень:** власники, засновники, акціонери	**2 рівень:** топ-менеджмент, дирекція	**3 рівень:** Весь персонал	**4 рівень:** Працівники окремих підрозділів	**5 рівень:** Працівники, відповідальні за окремі напрями роботи	**6 рівень:** Працівники бухгалтерського, аналітичного та планового відділів
1. Фінансова безпека	Фінансова стабілізація суб'єкта господарювання	Запобігання зниження прибутку, підвищення рентабельності	Підвищення мотивації персоналу в отриманні прибутку	Виконання вимог фінансової безпеки	Підвищення продуктивності праці	Контроль фінансово-господарської діяльності
2. Кадрова безпека	Фінансування системи професійної підготовки та перепідготовки кадрів	Вдосконалення кадрової політики, зменшення плинності кадрів	Виконання кваліфікаційних вимог професійної компетентності	Розробка кваліфікаційних вимог до персоналу	Кадрове забезпечення поточної діяльності	Облік і контроль підготовки працівників
3. Силова безпека	Фінансування розробки системи охорони	Розробка положення про фізичну охорону	Забезпечення захисту персоналу	Виконання режимних охоронних заходів	Виконання вимог підрозділів охорони	Аудит і контроль режиму охорони
4. Пожежна безпека	Фінансування засобів пожежного захисту	Розробка положення та організація пожежного захисту	Навчання персоналу користування пожежними системами	Монтаж систем пожежного захисту	Виконання вимог систем пожежного захисту	Контроль дотримання пожежної безпеки

5. Інформаційна безпека	Фінансування заходів протидії недобросовісної конкуренції в сфері інформаційної безпеки	Організація системи захисту комерційної таємниці	Навчання персоналу навикам інформаційної безпеки	Розробка стратегії інформатизації діяльності	Інформатизація діяльності	Аудит і контроль дотримання інформаційної безпеки
6. Екологічна безпека	Фінансування купівлі екологічно безпечного обладнання і технологій	Організація виробництва екологічно безпечної продукції	Участь у проектах з нормалізації екологічної ситуації	Виконання вимог екологічних нормативів	Проведення санітарно-гігієнічного моніторингу в процесі діяльності	Аналіз природо-охоронного законодавства
7. Технологічна безпека	Технологічне переозброєння	Технологічна модернізація виробництва у відповідності до міжнародних стандартів	Підготовка кадрів, що володіють сучасними технологіями	Підвищення конкурентно-спроможності виробництва	Реалізація заходів з впровадження сучасних технологій	Аудит в контроль впровадження сучасних технологій
8. Майнова безпека	Формування заходів нормативно-правового регулювання	Розробка і реалізація локальних положень з майнової безпеки	Підвищення кваліфікації персоналу з захисту активів	Оптимізація внутрішнього управління майновою безпекою	Виконання вимог охоронної діяльності	Облік і контроль над активами та основними засобами підприємства

Складено автором

За допомогою матриці можливо визначити сукупну величину попередження ризику, сумарні затрати на реалізацію заходів щодо попередження ризику і загальну величину понесених збитків відповідної функціональної складової. Обчислення вказаних показників відображає економічний ефект діяльності служб безпеки охоронних підприємств в процесі забезпечення економічної безпеки суб'єктів господарювання.

Ні в кого не викликає сумніву, що на сьогоднішній день для урегулювання розвитку ринку охоронної діяльності необхідною умовою є ухвалення відповідних змін до Закону України «Про охоронну діяльність» [3], що має стати одним з інструментів розвитку конкурентного ринку охоронних послуг на території України.

При розробці ряду законопроектів, пов'язаних з охоронною сферою, доцільно звернути увагу на позитивний досвід більшості країн Європейського Союзу, в яких таке законодавство створене давно, а даний сектор успішно розвивається по теперішній день.

При створенні законодавчої основи для ринку послуг охорони необхідно виконати наступні дії:

1. Провести дискусію з зацікавленою групою цього сегменту ринку. Якщо автори законопроекту дійсно бажають зробити умови для нормального розвитку цієї галузі, обов'язково повинен бути діалог учасників цього ринку, тобто дискусія має бути проведена між наступними групами:

– органи влади. При цьому це не лише Міністерство Внутрішніх справ України, а також і Антимонопольний комітет, Нацбанк, Міністерство надзвичайних ситуацій тощо;

– приватні учасники ринку. Це можуть бути асоціації та спілки, що представляють компанії, що займаються наданням охоронних послуг;

– найбільші споживачі. Мова йде насамперед про представників банківських установ, що протягом довгого відрізку часу виступають за врегулювання даної сфери.

При цьому необхідно щоб автори даного законопроекту відмовились від формального ставлення до зауважень та пропозицій інших учасників дискусії. Всі рішення повинні бути аргументованими.

2. Привести законопроект у відповідність з державною політикою розвитку бізнес-середовища. Окремого перегляду потребують положення Закону України «Про охоронну діяльність» [4], що ведуть до надмірного втручання в діяльність суб'єктів ринку.

При встановленні вимог щодо сертифікації, в Законі також повинні враховуватись ряд заходів, які здійснює влада для реформування системи технічного ліцензування та приведення її до норм, що діють в Європейському Союзі. При цьому передбачається скорочення обов'язкової сертифікації для деякого переліку послуг та продукції. Контролювати якість та безпеку мають спеціальні органи в рамках системи ринкового нагляду.

1. Створити рівні умови для чесної конкуренції. Для всіх учасників ринку Закон повинен створювати рівні умови для нормального розвитку та функціонування у відповідності до конституційних принципах рівності прав господарюючих суб'єктів.

Виключення з цього Закону можуть бути лише для охорони об'єктів підвищеної небезпеки, кількість який повинна обговорюватись в ході дискусії.

Для забезпечення чесної конкуренції та прозорості ринку охоронних послуг також необхідно мінімізувати негативні наслідки конфлікту інтересів Національної поліції охорони та приватних компаній, що надають охоронні послуги.

2. Створити необхідні умови для нормального захисту прав споживачів ринку охоронних послуг. Даний Закон має містити засади, що зможуть гарантувати права основних споживачів охоронних послуг.

3. Забезпечити для кожного споживача право вибору та доступність послуг. Для цього необхідно створити конкуренцію на ринку.

4. Гарантувати право на якість та безпеку наданих послуг. Таке право не може забезпечуватись забороною для приватних охоронних фірм на надання

послуг лише окремим категоріям споживачів ринку. Спеціально для цього повинно бути введене ліцензування та проводитись контроль за діяльністю охоронних компаній.

5. Надати право на захист своїх інтересів. Для цього Закон моє містити відповідні положення, що зможуть врегулювати відносини споживачів та організацій, що надають охоронні послуги. Мають бути чітко описані права, зобов'язання, відповідальність обох сторін.

Зважаючи на те, що відповідне економічне становище суб'єктів потребує відповідного захисту їх господарської діяльності, в Законі також повинні бути розглянути питання регламентації діяльності з забезпечення економічної безпеки.

Система економічної безпеки підприємства організовується та координується спеціальним органом, що є одним з підрозділів підприємства (чи залученою організацією на умовах аутсорсингу) – службою безпеки. Саме ця служба відповідає за питання організації безпеки суб'єкта господарювання. Насамперед, слід зазначити, що наявність на підприємстві повноформатної служби безпеки, котра застосовує у своїй роботі оперативно-технічні та процесуальні заходи, втручається у ті відносини, які є чіткою прерогативою лише деяких державних органів.

Останнім часом в Україні все частіше можна спостерігати зростання несумлінних підприємств-посередників фізичних осіб-боржників та шахраїв, що завдяки недосконалості чинного законодавства можуть наносити суттєві збитки підприємствам. Саме тому існує необхідність в залученні компетентних спеціалістів, проведенні аудиту і оцінки економічної безпеки суб'єктів господарювання.

Як наголошено в ст.4 Закону України «Про основи національної безпеки України» [5], суб'єктами забезпечення національної безпеки є об'єднання громадян. Теперішній час відсутнє залучення громадських об'єднань з метою забезпечення національної економічної безпеки. При цьому роль недержавних структур, що займаються виконанням таких функції, з кожним роком лише

збільшується. Діяльність же професійних громадських об’єднань, що займаються проблемами безпеки, повинна сприяти забезпеченню нацбезпеки України. Її необхідно розглядати як окрему складову, що є підсистемою в загальній системі національної безпеки України.

Результати вдосконалення нормативно-правової бази в сфері забезпечення економічної безпеки підприємств службами безпеки охоронних фірм повинні виглядати наступним чином:

– оптимізація систем суб’єктів та зміцнення кадрового потенціалу охоронної діяльності в Україні;

– вдосконалення нормативно-правової, матеріально-технічної, та науково-методичної бази функціонування діяльності охоронних фірм на території України;

– законодавче закріплення діяльності охоронних фірм в Україні через механізм саморегулювання. Це стосується розробки проекту Закону «Про охоронну діяльність» через механізм саморегулювання в Україні;

– заснування і підтримка інноваційних форм охоронної діяльності і Україні завдяки механізму саморегулювання.

При цьому також важливим завданням є визначення пріоритетних сфер реформування ведення діяльності з забезпечення безпеки охоронними компаніями та відповідальних за їх реалізацію.

В процесі діяльності охоронні підприємства почали все більше уваги приділяти економічній безпеці підприємств-замовників. Це зумовлено тим, що від рівня фінансової безпеки останніх залежить фінансова безпеки охоронних підприємств. Тому охоронні підприємства розширюють спектр послуг і будують ефективну систему безпеки на підприємствах, що охороняються.

В останні роки все частіше охоронний персонал розглядають як одну із складових системи забезпечення економічної безпеки. При цьому керівництво суб'єкта господарювання має чітко розуміти завдання, складність та ступінь надійності функціональних елементів та мати уявлення про роль охорони персоналу в роботі всієї системи безпеки.

Одним із основних завдань служби безпеки із забезпечення режиму та охорони є організація та здійснення заходів, що необхідні для гарантування безпеки діяльності та захисту інформації. При цьому можуть використовуватись всі можливі способи та засоби щодо їх здійснення.

Серед завдань організації режиму та охорони є:

– ряд заходів, що необхідні для запобігання проникненню сторонніх осіб до службових приміщень, на територію об’єкта та окремих його зон, що знаходяться під охороною;

– забезпечення порядку при внесенні (винесенні), ввезенні (вивезенні) матеріальних цінностей, а також при вході та виході працівників та клієнтів з охоронюваної території.

Всі приміщення на підприємстві чітко діляться в залежності від призначення, характеру здійснюваних дій чи операцій. При цьому виділяються кілька зон доступності (безпеки), які визначаються шляхом врахування їх ступенів важливості з огляду на можливі збитки від кримінальних загроз. Всі зони безпеки облаштовуються послідовно, починаючи від огорожі та закінчуючи сховищем цінностей та інформації. При цьому створюється свого роду ланцюг перешкод, що буде заважати зловмиснику досягнути поставленої мети.

1. Фінансова безпека.

До основних господарських процесів в яких, на думку експертів, втрати становлять 30% і більше, належать:

1) капітальне будівництво;
2) інвестиційні проекти
3) закупівля сировини та матеріалів;
4) розрахунки з підрядниками та приймання виконаних робіт.

Відповідно до Матриці управлінських рішень (табл. 2.4), загрози фінансової безпеки можна вирішувати на декількох рівнях. Фінансові рішення приймаються на першому рівні та можуть бути ініційовані на рівнях нижче.

Прийняття тендерних рішень повинно супроводжуватись незалежним аналізом цін і пропозицій. Для цього охоронні підприємства вводять відділ «Аналізу цін» до складу служб безпеки. А служба безпеки перевіряє легітимність всіх тендерних пропозицій. На рисунку 2.11 наведений приклад захисної моделі прийняття фінансових рішень, пов'язаних з бізнес-процесами, втрати в яких найбільші.

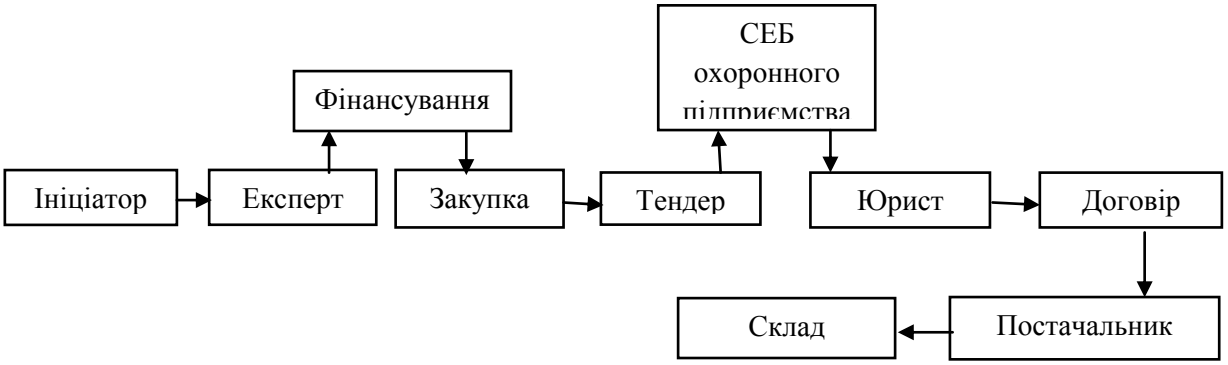


Рис. 2.11. Захисна модель процесу закупівель

Алгоритм захисту полягає в наступному:

1. Ініціатор ніколи не говорить, у кого купувати і за скільки.
2. Керівник ніколи не може ініціювати сам заявку.
3. У складі «експертної групи» немає нікого з підрозділу Ініціатора і сам склад групи непостійний, рішення колегіальне.
4. Той, хто готує тендер, не бере участі ні в ухваленні рішення, ні в самій закупівлі.
5. Ініціатор не здійснює приймання робіт за своєю заявкою.
6. Представник служби економічної безпеки - учасник проведення тендера.
7. Підготовлений тендер проходить експертизу.

Повна модель опрацьовується тільки з урахуванням специфіки конкретного підприємства, та з урахуванням внутрішньої етики.

2. Кадрова безпека.

Для реалізації концепцій та стратегій необхідне виконування цілого ряду конкретних заходів та механізмів, що були розроблені на основі аналізу

результату моніторингу якісних критеріїв та кількісних параметрів кадрової безпеки.

Максимальний ступінь економічної безпеки може бути досягнений лише за умови, що весь комплекс управлінських рішень реалізовується на всіх шести рівнях.

Кадрова безпека підприємства залежить не лише від зовнішніх (інфляція, тиск на співробітників), але й від внутрішніх факторів (недостатня кваліфікація особового складу, малоефективна система мотивації). Ці фактори обов'язково треба враховувати при аналізі стану кадрової роботи з точки зору безпеки щодо беззбитковості трудових відносин.

Для збереження кадрової безпеки службами безпеки охоронних фірм використовуються сучасні кадрові технології, що включають в себе такі механізми:

- ефективна мотивація;
- прискорена адаптація, що відбувається за рахунок наставництва;
- своєчасне реагування на конфліктні ситуації та запобігання ним;
- атестація;
- компенсація;
- пропаганда корпоративності;
- розумна політика звільнення.

3. Загрози силової безпеки

Надійна охорона матеріальних цінностей, конфіденційних документів та інформації, яка має відомості комерційного характеру, а також своєчасне запобігання спробам несанкціонованого доступу до них можлива лише при встановленні певного режиму діяльності, якого мають дотримуватись не лише все працівники, але й відвідувачі і клієнти підприємства.

Працівники та керівники фірм, що надають послуги охорони, мають чітко виконувати всі норми у відповідності до чинного законодавства, нормативних документів та певних рекомендацій. Види зон режимності фірми наведено в табл. 2.5.

Таблиця 2.5

Класифікація зон режимності фірми

Категорія режиму доступу	Назва	Функціональне призначення	Умови доступу працівників	Умови доступу відвідувачів	Наявність охорони	Наявність технічних засобів охорони
0	Вільна	Зона вільних відвідувань	Вільний	Вільний	Ні	Ні
1	Спостер ежувана	Зона прийому відвідувачів	Вільний	Вільний	Обмежена	Засоби спостереження і запису
2	Реєстрац ійна	Зона службових приміщень і кабінетів працівників	Обмежений службовою необхідністю	Реєстрований, З разовими перепустками	У 8 окремих зонах	Засоби охорони і контролю
3	Режимна	Зона керівного складу, спеціальних підрозділів фінансових служб	Суворо обмежений	Реєстрований, З разовими перепустками із супроводом	Посилена багатозонн а	Засоби охорони, контролю і спостереження

Складено автором

Організація контрольно-пропускного режиму має цілий ряд складнощів. Взагалі такий механізм зумовлений введенням в дію певних заборон та обмежень для суб’єктів, що перетинають межі об’єктів, що знаходяться під охороною. Все це здійснюється для забезпечення інтересів підприємства і вимагає чіткого виконання всіх вимог чинного законодавства.

4. Загрози пожежної безпеки

Варто відмітити факт, що майже все охоронні фірми мають необхідну ліцензію, що дозволяє надавати послуги з монтажу та обслуговування пожежних систем. Такі системи мають запобігати негативному впливу на людей факторів, що виникають в разі пожежі чи їх вторинних проявів. Основні напрямки забезпечення пожежної безпеки — ліквідація будь-яких чинників, що можуть викликати пожежу та мінімізація наслідків від можливих пожеж.

Відповідно до Мартиці управлінських рішень пожежна безпека стосується всіх шести рівнів, починаючи від звичайних робітників, закінчуючи власниками та акціонерами підприємства.

5. *Загрози інформаційної безпеки.*

Підприємством разом зі службами безпеки охоронних фірм розробляється і впроваджується відповідний комплекс заходів, що необхідні для ефективного захисту конфіденційних даних та інформаційних процесів. Такий механізм передбачає введення відповідних вимог до персоналу, менеджерів, технічних служб підприємства.

Основні етапи побудови політики інформаційної безпеки:

1) реєстрація всіх документів та інформації, що має бути захищена;
2) аналіз і створення списку можливих загроз для всіх типів ресурсів;
3) оцінка імовірності появи кожної з загроз;
4) вжиття заходів, що дозволять економічно ефективно забезпечити захист інформаційної системи.

Як відмічають спеціалісти в цій галузі, інформаційна безпека може бути на належному рівні лише у випадку, коли для всіх інформаційних ресурсів підтримується необхідний рівень конфіденційності, цілісності та доступності.

Серед підсистем ефективного захисту інформації можна виділити наступні:

1. Підсистема антивірусного захисту при користуванні мережею Інтернет, файлових серверів на робочих місцях працівників, централізованого управління. При цьому необхідно періодично оновлювати бази даних антивірусних програм.

2. Підсистема управління контролем доступу та ідентифікацією в інформаційній системі.

3. Підсистема криптографічного захисту. З її допомогою безпека передачі інформації гарантується завдяки використання спеціальних шифрувальних кодів.

4. Підсистема міжмережного екранування. Вона дозволяє забезпечити безпеку міжмережної взаємодії завдяки використанню програмних та програмно-апаратних межмережових екранів.

5. Підсистема захисту мобільних пристроїв.

6. Підсистема захисту систем управління базами даних.

7. Підсистема захисту від інсайдерів. З її допомогою відбувається контроль дії порушників, а сама інформаційна безпека реалізується при управлінні доступом та реєстрації.

8. Підсистема забезпечення цілісності інформації та програмного середовища. Реалізується вона шляхом використання відповідних засобів, що призначені для контролю і фіксації стану програмного комплексу, управління зберіганням інформації для резервного копіювання і архівування.

9. Підсистема виявлення спроб несанкціонованого доступу до інформаційних ресурсів підприємства. За допомогою даної підсистеми вдається провести ряд заходів, що зможуть надійно протидіяти атакам хакерів та поширенню спаму.

10. Підсистема моніторингу подій інформаційної безпеки. Така підсистема допоможе своєчасно виявити загрози інформаційним ресурсам та оперативно зреагувати на них.

Для забезпечення високої ефективності ведення підприємницької діяльності варто постійно проводити ряд заходів для підтримки інформаційної безпеки на належному рівні.

6. Загрози екологічної безпеки

Служби безпеки немалу увагу приділяють і екологічній безпеці, зокрема на промислових підприємствах.

В ході господарської діяльності підприємство може стати великою небезпекою для навколишнього середовища та людей зокрема. Серед внутрішніх чинників, що впливають на екологічну безпеку, можна виділити: помилки, що були зроблені при проектуванні і які є шкідливими для здоров’я людей; штрафи, які можуть бути виписані за забруднення довкілля, створення звалищ в неналежних місцях тощо.

Екологічна складова потребує дотримання чинних екологічних норм, мінімізації втрат від забруднення середовища.

Відповідно до загальних стратегічних рекомендацій щодо забезпечення комплексної безпеки, залученими службами безпеки при співпраці з керівництвом підприємства розробляється цілий комплекс заходів, що необхідні для забезпечення екологічної складової економічної безпеки в майбутньому. Даний план є лише частиною програми забезпечення належного рівня економічної безпеки. Виражений він як комплекс заходів, що відбуваються у певній послідовності з додаванням розрахунку ефективності практичного застосування даних заходів.

Алгоритм процесу забезпечення екологічної безпеки підприємства включає в себе ряд дій, проведених в наступній послідовності:

1) розрахунок карти ефективності проведених заходів для забезпечення екологічної складової економічної безпеки підприємства;

2) аналіз проведених розрахунків та розробка рекомендацій, що мають підвищити ефективність здійснюваних заходів;

3) розробка альтернативних сценаріїв відносно реалізації запланованих заходів;

4) вибір пріоритетного сценарію. Це відбувається на основі порівняння здійснених розрахунків;

5) подання обраного сценарію, що входить до складу загального плану гарантування економічної безпеки, до підрозділів, які займаються функціональним плануванням фінансово-господарської діяльності підприємства;

6) практичне виконання запланованого ряду заходів безпосередньо в процесі функціонування підприємства.

7. Загрози технологічної безпеки.

Ряд заходів для забезпечення технологічної безпеки на підприємстві є одним із найголовніших. Технологічна безпека підприємства (ТБП) полягає у порівнянні рівня застосованих технологій, що використовуються на підприємстві, з найкращими світовими аналогами за оптимізації ціни. Серед негативних впливів на цю складову варту виділити:

– дії, що спрямовані на підрив технологічного потенціалу компанії;

– порушення технологічної дисципліни;

– використання застарілих технологій.

До зовнішніх загроз послаблення ТБП відносяться брак зовнішніх та внутрішніх інвестицій. До то ж слід підкреслити труднощі, що часто виникають при потребі довгострокового кредиту від банку. Через це практично не відбувається поповнення обігових коштів, що повинні спрямовуватись на оновлення парку обладнання підприємства.

Що стосується технологічної складової економічної безпеки, то процес її забезпечення зазвичай відбувається в декілька етапів. В першу чергу проводиться аналіз ринку технологій у виробництві продукції, що відбувається аналогічно профілю певного підприємства чи організації проектувальника. При цьому проводиться аналіз:

– інформації про особливості технологічних процесів;

– науково технічної інформації щодо нових розробок в конкретній галузі;

– технологій, що спроможні здійснити інтервенцію на галузевий технологічний ринок.

Наступний етап – аналіз конкретних технологічних процесів. При цьому також відбувається виявлення внутрішніх резервів для покращення використовуваних технологій.

Третій етап включає в себе виконання наступних дій:

а) аналіз товарних ринків за профілем продукції, що виготовляє підприємство, та ринків товарів-замінників;

б) проводиться оцінка перспектив розвитку ринку продукції підприємства;

в) прогнозується можлива специфіка необхідних технологічних процесів, що необхідні для виготовлення конкурентоспроможних товарів.

Четвертий етап характеризується розробкою технологічних стратегій розвитку підприємства, а саме:

1) проводять ряд дій для виявлення перспективних товарів з групи, що виготовляється на підприємстві;

2) планується комплекс технологій, що необхідні для виробництва перспективних товарів;

3) проводять оцінку бюджету, що необхідний для розвитку підприємства. Це відбувається на основі витрат за програмою технологічного розвитку, опрацювання власних розробок чи за рахунок придбання патентів та необхідного для ефективної роботи устаткування;

4) розробляється загальний план технологічного розвитку підприємства. При цьому відображаються альтернативний варіант технологічного розвитку, обсяг фінансування, яке потрібне для цього, відповідальні виконавці.

5) складається план власних корпоративних ресурсів відповідно до плану технологічного розвитку підприємства.

В ході виконання п’ятого етапу відбувається оперативна реалізація планів технологічного розвитку підприємства і процесі його функціонування.

На завершальному етапі відбувається аналіз результатів практичного виконання заходів по забезпеченню техніко-технологічної складової економічної безпеки. При цьому беруться до уваги результати спеціальної карти розрахунків ефективності задіяних заходів.

Відповідно до Матриці управлінських рішень, заходи щодо попередження загроз технологічної безпеки можна згрупувати відповідно до рівнів безпеки (рис 2.12).

8. Загрози майнової безпеки.

Прохід на територію об’єкта здійснюється через спеціально оздоблені для цього контрольно-пропускні пункти. При цьому потрапити на територію підприємства можуть як працівники, так і відвідувачі при пред’явленні перепустки, що є основним документом, що дає право на прохід.

Варто відмітити і обмежений допуск працівників на територію підприємства у святкові, вихідні дні чи неробочий час. Це відбувається за попередніми заявками чи списками, що складаються керівниками підрозділів, при пред’явленні перепустки. На тих об’єктах, де є змінний режим роботи, при необхідності до перепусток додаються і спеціальні вкладки змінності.

Рішення з забезпечення технологічної безпеки

1 рівень: власники, засновники, акціонери	**2 рівень:** топ-менеджмент, дирекція	**3 рівень:** Весь персонал	**4 рівень:** Працівники окремих підрозділів	**5 рівень:** Працівники, відповідальні за окремі напрями роботи	**6 рівень:** Працівники бухгалтерського, аналітичного та планового відділів
Технологічне переозброєння	Технологічна модернізація виробництва у відповідності до міжнародних стандартів	Підготовка кадрів, що володіють сучасними технологіями	Підвищення конкурентно-спроможності виробництва	Реалізація заходів з впровадження сучасних технологій	Аудит в контроль впровадження сучасних технологій

Рис. 2.12. Заходи щодо попередження загроз технологічної безпеки

Складено автором

Чергові, що працюють позмінно у спеціальних службах підприємства, можуть бути допущені на територію об’єкта в неробочий час, а також в вихідні та святкові дні за списками, що заздалегідь складаються та підписуються начальниками відповідних служб. Список при цьому має також бути затверджений начальником служби безпеки.

Згідно з чинним законодавством та рішення адміністрації деякі категорії осіб можуть користуватись правом входу на об’єкт лише за пред’явленням службового посвідчення. Це стосується:

– працівників прокуратури;

– працівників міліції за територіальністю;

– інспекторів праці, котлонагляду, енергонагляду;

– всі посадові особи та деякі категорії працівників санітарно-епідеміологічної служби, що можуть здійснювати санітарний огляд об’єкта.

Категорії осіб, що можуть пройти на територію підприємства без пред’явлення перепустки, повинні бути внесені до інструкції про контрольно-пропускний режим.

Для забезпечення пропускного режиму на підприємстві та в його структурних підрозділах директор затверджує перелік підрозділів чи приміщень, яким присвоюється відповідна категорія. В таких приміщеннях діє спеціальний режим і підвищена відповідальність за його дотримання працівниками підрозділів. Допуск туди відбувається за списками, що узгоджується зі службою безпеки. Приймання в цих приміщеннях відвідувачів від сторонніх організацій та підприємств максимально обмежується. В кожному з таких приміщень вивішується список працівників, що мають відповідний допуск. В кінці зміни територія оглядається черговим підрозділу або особами, що відповідальні за протипожежний стан. По закінченню робочого дня такі приміщення закриваються, опечатуються та здаються під охорону. При цьому відбувається перевірка сигналізації працівником охорони в присутності працівників, що працюють і відповідному підрозділі. Ключі від приміщення здаються під розписку начальнику караулу.

Отримати ключі до приміщення, що знаходиться під сигналізацією, можуть лише особи, що мають доступ до конкретного приміщення та за пред'явлення постійної перепустки. Список таких працівників із вказанням номерів карток, які використовуються при опечатуванні приміщення, та номерів службових телефонів складає та підписує начальник підрозділу, затверджує начальник служби безпеки.

При спробі проникнути на територію підприємства без пред'явлення перепустки, використовуючи чужу чи неправильно оформлену перепустку, при намаганні пронесення на об'єкт (з об'єкта) заборонені предмети такі особи затримуються та передаються працівникам служби безпеки підприємства. При цьому начальник охорони чи черговий по об'єкту складає службову записку по кожному з таких порушень пропускного режиму.

Проїзд на територію (з території) об'єкта, що знаходиться під охороною транспортних засобів відбувається за пред'явленням водієм особистої перепустки, що містить спеціальний шифр, або транспортної перепустки та

дорожнього листка. Допуск вантажників та осіб, що супроводжують транспорт, відбувається через КПП на загальних підставах.

Транспортні засоби під час в'їзду чи виїзду з території підприємства оглядаються в обов'язковому порядку. В'їзд на власному транспорті працівників підприємства та стоянка на території охоронюваного об'єкту можлива лише за спеціальними списками.

Автотранспорт інших організацій, який прибув з вантажем на адресу охоронюваного підприємства в робочий час, допускається на територію за службовими записками, при проходженні обов'язкового огляду на транспортному КПП.

Що стосується залізничного транспорту і бригад, що займаються його супроводженням, допуск на територію об'єкта відбувається за перепустками встановленого зразка, за списками чи іншими документами, за зазначені в інструкції про пропускний режим.

Пропуск опломбованих вагонів відбувається лише після детального їх огляду на КПП. При цьому відтиски пломб повинні відповідати відтискам, що зазначені у супровідних документах чи накладних. Якщо ж виявлено невідповідність відтиску, пролом вагона (контейнера) чи обрив пломби, сам вагон (контейнер) розкривають на місці та оглядають в присутності представників адміністрації та залізниці.

Внесення чи винесення готової продукції чи інших матеріальних цінностей з території об'єкту відбувається за матеріальними перепустками встановленого зразка. Список документів на матеріальні цінності, які вивозяться чи виносяться з об'єкта, реєструють у бюро перепусток в книзі обліку. Ця інформація далі передається до бухгалтерії.

Документи на вивезення (винесення) матеріальних цінностей повинні бути вписані лише на ту кількість вантажу, що може бути вивезена (винесена) одночасно. Вони мають бути дійсні лише в конкретну дату, що обов'язково вказується у дозвільному документі. При цьому спеціалісти рекомендують вивозити металобрухт, будівельні відходи, макулатуру, металеву стружку як

матеріальні цінності з відповідним оформленням документів. При вивезенні сміття, снігу чи землі оформлення документів не є обов'язковим, при цьому водій має здійснити реєстрацію на транспортному КПП.

Отже, зробивши висновки, можна сміливо стверджувати, гарантування безпеки підприємства напряму залежить від системи контрольно-пропускного режиму. При цьому будь-яка система безпеки об'єкта від загроз повинна мати специфічну систему їх ідентифікації за принципом «свій-чужий» чи за рівнем доступу для захисту об'єкта та людей, що на ньому працюють, від небезпечних чинників.

Завдяки грамотній організації системи контрольно-пропускного режиму забезпечується не лише безпека підприємства, але й раціональна організація праці.

Всі організаційно-адміністративні заходи та інженерно-технічні рішення в системі контрольно-пропускного контролю можуть бути здійснені лише при наявності зв'язку з іншими елементами системи безпеки.

Роль контрольно-пропускного режиму в системі безпеки переоцінити достатньо важко. При організації такого пункту контролю необхідно застосовувати комплексний підхід до розроблення заходів обмеження доступу на територію об'єкта.

При вирішенні завдань протидії загрозам слід розглядати сукупність всіх елементів такої системи, а саме:

– дії підрозділів охорони;
– технічні рішення;
– організацій-адміністративні заходи.

При розробці систем контрольно-пропускного режиму варто застосовувати комплексний підхід, враховуючи значну кількість аспектів. Завдяки цьому можна буде уникнути немалих витрат часу та ресурсів, що необхідні при створенні інтегрованої системи безпеки підприємства.

На основі реалізації дій, що зменшують вплив загроз економічній безпеці та реалізації механізму забезпечення економічної безпеки службами безпеки

охоронних підприємств проведений повторний розрахунок відносної оцінки складових економічної безпеки. Показник індивідуального функціонального критерію рівня забезпечення функціональної складової економічної безпеки наведено в таблиці 2.6.

Таблиця 2.6

Повторний розрахунок відносної оцінки функціональних складових економічної безпеки суб'єктів господарської діяльності

Галузь підприємства - Назва	Функціональні складові безпеки підприємства								Сукупний критерій економічної безпеки
	Фінансова	Кадрова	Силова	Пожежна	Інформаційна	Екологічна	Технологічна	Майнова	
Виробництво – ПАТ «Азот»	2,70	3,52	2,50	3,80	1,78	2,87	3,10	2,32	22,59
Торгівля – ТОВ «Епіцентр К»	2,56	3,87	3,21	3,56	4,18	3,14	5,18	3,76	29,46
Банківські послуги – ПАТ «Укрінбанк»	5,98	3,22	4,33	3,45	2,67	3,44	3,45	5,21	31,75
Посередництво – АН «Бізнес Партнер»	4,33	3,89	2,15	2,99	3,56	3,12	3,11	5,18	28,33
Послуги – ТОВ «Делівері»	5,66	3,67	4,76	3,51	4,33	2,18	2,11	4,18	30,40
Охорона здоров'я – Клініка «Борис»	4,23	3,76	3,51	3,51	4,82	2,87	4,14	4,95	31,79
Будівництво – ТОВ «Добробуд»	4,33	2,43	3,58	4,23	3,53	2,32	2,67	3,85	26,94
Консалтингові послуги – КА «Персонал»	3,11	2,68	2,98	2,59	3,52	3,11	2,10	4,15	24,24
Сільське господарство – ТОВ «АПК «Маїс»	4,18	3,32	5,10	4,23	4,68	3,67	2,99	4,15	32,32
Засоби масової інформації – ТОВ «СТБ»	4,12	4,71	3,46	3,18	4,18	2,56	2,67	3,56	28,44

Джерело: розрахунки автора

За результатами розрахунків приватного функціонального критерію можна зробити висновок, що за допомогою запропонованих методів рівень економічної безпеки збільшився за усіма функціональними складовими. У таблиці 2.7 відображено відхилення величини сукупного критерію економічної безпеки у порівнянні з обчисленнями [6].

Таблиця 2.7

Відхилення величини сукупного критерію економічної безпеки суб'єктів господарської діяльності

Галузь підприємства - Назва	Початкова величина сукупного критерію ЕБ	Кінцева величина сукупного критерію ЕБ	Відхилення	
			+/-	%
Виробництво – ПАТ «Азот»	17,70	22,59	+4,89	27,63
Торгівля – ТОВ «Епіцентр К»	21,95	29,46	+7,51	34,21
Банківські послуги – ПАТ «Укрінбанк»	21,76	31,75	+9,99	45,91
Посередництво – АН «Бізнес Партнер»	19,37	28,33	+8,96	46,26
Послуги – ТОВ «Делівері»	22,19	30,40	+8,21	37,00
Охорона здоров'я – Клініка «Борис»	24,82	31,79	+6,97	28,08
Будівництво – ТОВ «Добробуд»	21,78	26,94	+5,16	23,69
Консалтингові послуги – КА «Персонал»	20,72	24,24	+3,52	16,99
Сільське господарство – ТОВ «АПК «Маїс»	24,22	32,32	+8,10	33,44
Засоби масової інформації – ТОВ «СТБ»	19,31	28,44	+9,13	47,28

Джерело: розрахунки автора

Порівняння динаміки величини сукупного критерію економічної безпеки у порівнянні з обчисленнями, показано на рис. 2.13

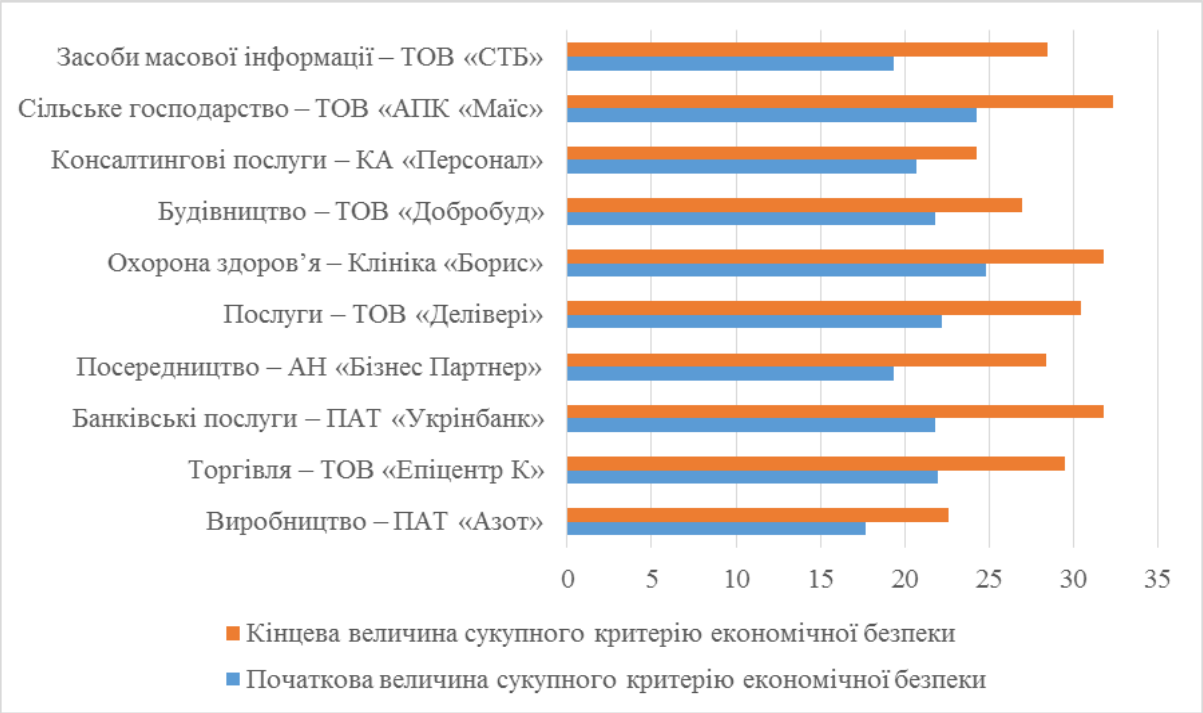


Рис. 2.13. Динаміка величини сукупного критерію економічної безпеки

Складено автором

Отже, провівши обчислення затрат на заходи запобігання загрозам, їх реалізацію та вартості понесених збитків після застосування та реалізації механізму забезпечення економічної безпеки службами безпеки охоронних підприємств можна зробити висновок, що рівень економічно безпеки підприємств галузей, що брали участь у дослідженні підвищився.

Механізм забезпечення економічної безпеки службами безпеки охоронних підприємств повинен стати дієвим інформаційно-аналітичним інструментом формування високого рівня системи економічної безпеки та оцінки її за функціональними складовими. Показник сукупного критерію економічної безпеки може мати практичне застосування як для внутрішнього використання (визначення працівниками та власниками суб'єктів господарювання міри їх захищеності), так і для зовнішнього (під час розрахунків спеціалістами служб безпеки охоронних підприємств), при вартісному відображенні впливу загроз різного характеру.

Список використаних джерел:

1. *Міненко М.В. Розробка механізму забезпечення економічної безпеки службами безпеки охоронних підприємств / Мігус І.П., Міненко М.В. // Бізнес-інформ - №6. 2015. – С.54-59.*
2. *Міненко М.В. Особливості прийняття управлінських рішень з попередження загроз економічній безпеці / Мігус І.П., Міненко М.В. // Перспективи управлінської діяльності суб'єктів господарювання в контексті економічної безпеки: Збірник тез доповідей учасників III Міжнародної науково – практичної конференції, Черкаси, 27-28 березня 2015 р. – Черкаси: вид-во ПП Чабаненко Ю.А., 2015. – 374 с.*
3. *Калінін Р. Недержавна служба безпеки України / Р. Калінін // Служба безпеки. – 1996. – №10. – С. 18-19.*
4. *Про охоронну діяльність Закон України // Відомості Верховної Ради України (ВВР), 2013, № 2, ст.8)*
5. *Про основи національної безпеки України Закон України від 19 червня 2003 р. № 964 - IV // Офіційний вісник України. – № 29. –38 с.*
6. *Міненко М.В. Забезпечення економічної безпеки суб'єктів господарювання службами безпеки охоронних підприємств :* дис... канд. екон. наук: 21.04.02 /М.В. Міненко ; Черкаський нац.-й ун-т. — Черкаси, 2015. — 207 с. [Електронний ресурс] Режим доступу до тексту : *chttps://drive.google.com/file/d/0Bz9Pblt6U8UmNEFmTVI5aDY5ODA/view.*

2.4. ОРГАНІЗАЦІЯ СИСТЕМИ ФІНАНСОВОГО МОНІТОРИНГУ В КОМЕРЦІЙНИХ БАНКАХ

ДМИТРОВ СЕРГІЙ ОЛЕГОВИЧ, *д.т.н., професор,*
ЗАНОРА ВОЛОДИМИР ОЛЕКСАНДРОВИЧ, *к.е.н., доцент*
кафедри менеджменту та економічної безпеки,
ДУДЧЕНКО НАТАЛІЯ ВАСИЛІВНА*, к.е.н., доцент,*
кафедри менеджменту та економічної безпеки
Черкаський національний університет імені Богдана Хмельницького

Правовими актами, що регулюють процес здійснення фінансового моніторингу в комерційних банках є Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму» від 14.10.2014 р. №1702-VII (далі – Базовий Закон), Закон України «Про банки і банківську діяльність» від 07.12.2000 р. № 2121-III, Постанова Правління Національного банку України від 26.06.2015 р. № 417 «Положення про здійснення банками фінансового моніторингу», Постанова Правління Національного банку України від 04.06.2003 р. № 233 «Про затвердження Складу реквізитів та структури файлів інформаційного обміну між спеціально уповноваженим органом виконавчої влади з питань фінансового моніторингу та банками (філіями)» та ін.

Функціонування фінансово-кредитної системи передбачає оперування, серед інших основних, поняттям «відмивання грошей». Відповідно до наявного світового досвіду – це процес, що пов’язаний з приховуванням джерел походження коштів, отриманих незаконним шляхом (або коштів, отриманих законним шляхом, але призначених для використання в незаконних цілях).

За своєю сутністю це злочинна діяльність, що характеризується різноманітністю ймовірних етапів її провадження. Вона є основною при цілеспрямованій підтримці наркоторгівлі, нелегальної міграції, при фінансуванні членів злочинних угрупувань, осіб, які торгують інсайдерською інформацією, а також інших, які б хотіли уникнути уваги до себе, викликаної «раптовою» появою грошей на рахунку в банку.

Жодна фінансово-кредитна установа не застрахована від ймовірності випадкової співучасті в процесі відмивання грошей, а тому впровадження комплексу заходів фінансового моніторингу на рівні окремої банківської установи та, в цілому, вітчизняної фінансово-кредитної системи є необхідним та обґрунтованим з огляду на вимоги світового співтовариства.

Організація внутрішньобанківської системи по запобіганню легалізації (відмивання) доходів, одержаних злочинним шляхом, представлена на рисунку 2.14.

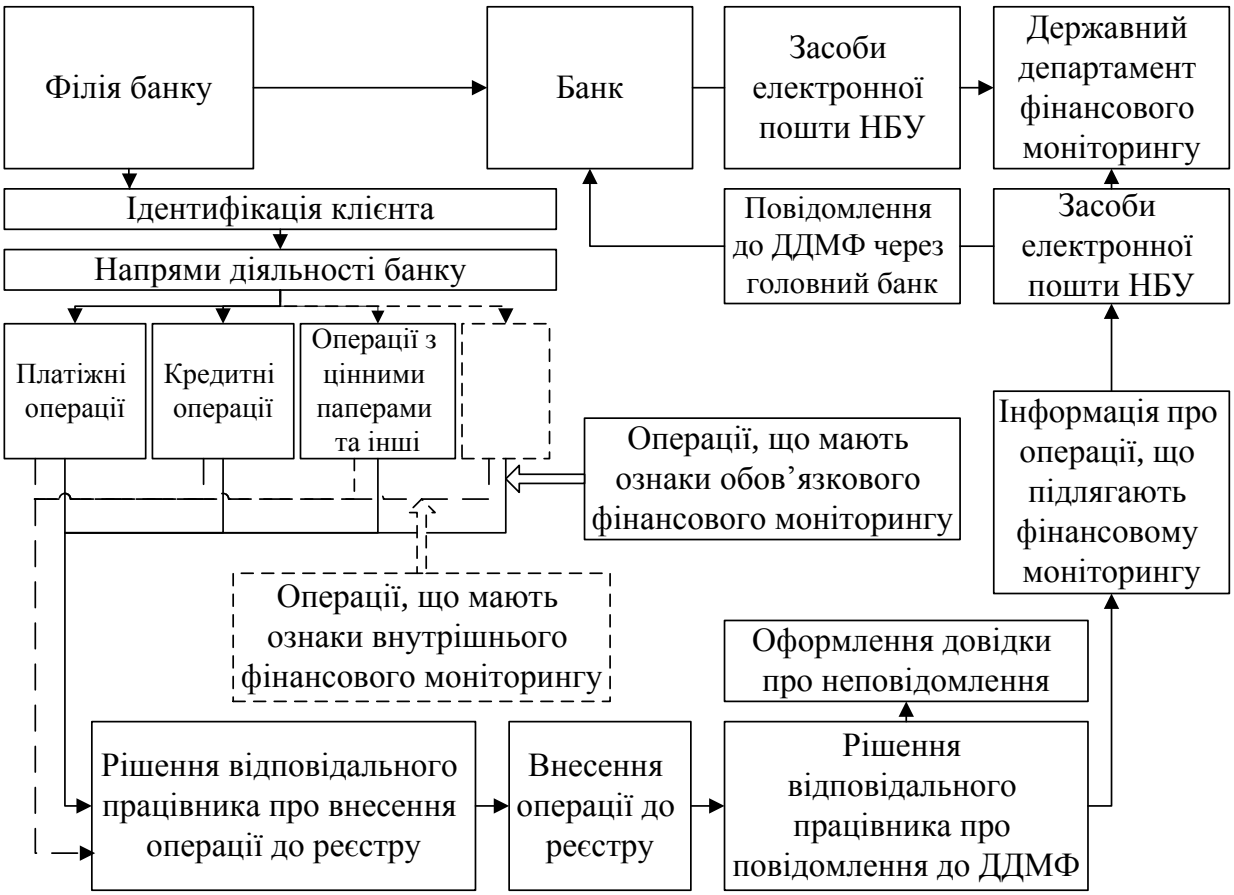


Рис. 2.14. Структурно-логічна схема фінансового моніторингу в банку

Організаційна структура внутрішньобанківської системи запобігання легалізації доходів, одержаних злочинним шляхом, складається з таких складників:

1. Відповідального за систему;

2. Керівників та працівників перелічених нижче відділів банку, які безпосередньо обслуговують клієнтів та беруть участь у здійсненні фінансового моніторингу: відділ обслуговування корпоративних клієнтів; відділ обслуговування фізичних клієнтів; відділ валютного контролю; відділ загального кредитування; відділ платіжних систем; відділ управління цінними паперами; юридичний департамент.

Система організації фінансового моніторингу в банку складається з наступних рівнів: 1 рівень – працівники та відділи, які обслуговують клієнтів; 2 рівень – адміністратор з питань дотримання внутрішніх процедур; 3 рівень – відповідальна особа банку.

На першому рівні співробітники, які проводять операції з клієнтами за відповідними напрямами діяльності, аналізують та виявляють фінансові операції, що підлягають обов'язковому та внутрішньому фінансовому моніторингу. Якщо працівник Банку перед або після здійснення фінансової операції вважає, що вона підлягає фінансовому моніторингу, то він усно (з дотриманням вимог конфіденційності) повідомляє про таке адміністратора з питань дотримання внутрішніх процедур, а також не пізніше 12 годин наступного робочого дня повідомляє про це через внутрішньобанківську пошту.

Адміністратор з питань дотримання внутрішніх процедур переглядає включені до реєстру фінансові операції, що виявлені за допомогою програмного забезпечення, а також працівниками Банку, та готує інформацію відповідальній особі для прийняття рішення про реєстрацію фінансових операцій та направлення інформації до Уповноваженого органу.

На заключному, третьому рівні, відповідальний працівник Банку приймає остаточне рішення щодо реєстрації операцій отриманих від адміністратора внутрішніх процедур та щодо надання інформації про такі операції до ДСФМУ (Державна служба фінансового моніторингу України).

Банк працює в системі консолідованих повідомлень через Головний офіс банку. Робоче місце для формування файлів-повідомлень до ДСФМУ та прийому файлів-квитанцій створено у Відділі фінансового моніторингу Головного офісу Банку. Програмне забезпечення надає можливість у робочому режимі програми автоматично надсилати файл-повідомлення, отримувати файл-повідомлення про взяття (відмову від взяття) фінансової операції (фінансових операцій) на облік від ДСФМУ, обробляти отриманий файл та вносити корективи, у разі наявності помилок.

Отже, організація первинного фінансового моніторингу в першу чергу покладається на уповноваженого працівника, а досягнення ефективного його впровадження залежить від повного дотримання правил та порядку здійснення самої процедури проведення внутрішнього фінансового моніторингу. Інформація, отримана на цьому рівні системи запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом, є відправним пунктом для здійснення обов’язкового фінансового моніторингу на рівні уповноваженого органу.

Світова практика визнає за необхідне, щоб суб’єкти первинного фінансового моніторингу, зокрема комерційні банки, мали в своєму розпорядженні повну інформацію щодо своїх клієнтів, з якими вони мають справу.

Відповідне належне ставлення до нових та вже існуючих клієнтів є основою всіх діючих правил контролю. Невідповідність стандартам «Знай свого клієнта» (далі – ЗСК (англ. KYC)) або їх відсутність може зумовити реалізацію ризиків з боку клієнта й протилежної сторони, особливо під ризик репутації, концентрації, операційний та юридичний ризики. Варто зазначити, що всі ці ризики взаємопов’язані та є складними, проте, будь-який з них може в результаті реалізації призвести до значних фінансових збитків банківської установи.

Комерційні банки розробляють чіткі політику та процедури прийняття клієнтів, в тому числі опис типів клієнтів, які характеризуються більшим за

звичайний ступенем ризику для них. Під час розробки такої політики вивчають такі показники як загальний профіль клієнта, країна походження, соціальний статус або стосунки з органами влади, пов'язані з ним рахунки, ділову активність та інші чинники ризику.

Згідно діючого законодавства України банк зобов'язаний здійснювати ідентифікацію та вивчення клієнта у випадках, установлених законом.

Ідентифікація клієнта здійснюється до/або під час встановлення ділових відносин, укладення правочинів, але до проведення фінансової операції, відкриття рахунку, у разі:

- встановлення ділових відносин з клієнтами;

- виникнення підозри в тому, що фінансова операція може бути пов'язана з легалізацією (відмиванням) доходів, одержаних злочинним шляхом, або фінансуванням тероризму;

- проведення фінансової операції, що підлягає фінансовому моніторингу;

- проведення разової фінансової операції без встановлення ділових відносин з клієнтами на суму, що дорівнює чи перевищує суму, що визначена Базовим законом.

Ідентифікація здійснюється на підставі поданих офіційних документів або засвідчених в установленому порядку їх копій, а також додаткових даних для вивчення клієнта, що можуть бути одержані від клієнта, а також з інших джерел, якщо така інформація є публічною (відкритою). Документи мають бути чинними на момент їх подання та включати всі необхідні дані для ідентифікації. У разі виникнення сумнівів у достовірності чи повноті наданої інформації про клієнта банк зобов'язаний вжити заходів для перевірки та уточнення інформації стосовно ідентифікації такого клієнта (особи).

Банк має право витребувати, а клієнт зобов'язаний надати інформацію стосовно: ідентифікації його особи, змісту його діяльності; фінансового стану.

У разі якщо особа діє як представник іншої особи, банк повинен перевірити окрім відповідних ідентифікаційних даних наявність у цієї особи відповідних повноважень.

У тому випадку, якщо у банку виникає сумнів стосовно того, що особа виступає не від власного імені або вигодоодержувачем є інша особа, то банк зобов'язаний ідентифікувати також особу, від імені або за дорученням чи в інтересах якої проводиться фінансова операція або яка є вигодоодержувачем.

У разі ненадання клієнтом, з яким встановлені ділові відносини, необхідної інформації для ідентифікації та вивчення фінансової діяльності банк має право відмовити йому в проведенні подальших фінансових операцій.

Ідентифікація клієнта не є обов'язковою у разі проведення фінансової операції особами, які раніше були ідентифіковані, укладення правочинів між банками, зареєстрованими в Україні.

Дані, які повинні бути встановлені банками з метою ідентифікації клієнтів представлені в табл. 2.8.

Банк може здійснити спрощену ідентифікацію клієнтів, віднесених до типу клієнтів із низьким ризиком, що передбачає отримання зменшеного переліку відомостей для ідентифікації з відповідними підтверджуючими документами, у разі:

- встановлення ділових відносин або проведення фінансової операції, якщо клієнтом виступає орган державної влади, підприємство, що повністю перебуває у державній власності;

- міжнародна установа чи організація, в яких бере участь Україна відповідно до міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України;

- проведення фінансової операції на організованому ринку цінних паперів.

Таблиця 2.8

Ідентифікаційні дані

Тип клієнта	Ідентифікаційні дані (відомості)	
	резидент	**нерезидент**
Фізична особа	ПІБ	
	Дата народження	
	Серія і номер паспорта (або іншого документа що посвідчує особу)	
	Дату видачі паспорта (або іншого документа що посвідчує особу)	
	ІН або серію та номер паспорту в якому проставлено відмітку органів державної податкової служби про відмову від одержання ІК	
		громадянство
Фізична особа-підприємець	ПІБ	
	Дату народження	
	Серія і номер паспорта (або іншого документа що посвідчує особу)	
	Дату видачі паспорта (або іншого документа що посвідчує особу)	
	Орган, що видав паспорт (або інший документ що посвідчує особу)	
	Місце проживання або місце перебування	
	Реквізити свідоцтва про державну реєстрацію	
	Орган що видав свідоцтво про державну реєстрацію	
	Реквізити банку в якому відкрито рахунок (за наявності)	
	Номер банківського рахунку (за наявності)	
Юридична особа	Повне найменування	
	Місце знаходження	
	Реквізити свідоцтва про державну реєстрацію	
	Орган що видав свідоцтво про державну реєстрацію	
	Відомості про орган управління та їх склад	
	Дані, що ідентифікують осіб, які мають право розпоряджатися рахунками і майном	
	Відомості про власників істотної участі в юридичній особі	
	Відомості про контролерів юридичної особи	
	КОД ЄДРПОУ	
	Реквізити банку в якому відкрито рахунок	
	Номер банківського рахунку	

До основних джерел отримання інформації при вивченні клієнтів відносяться:

- різноманітні бази даних для здійснення комплаєнсу (World Check);
- економічні бази даних (Global Monitor);
- друковані джерела;

- регіональні бази даних;

- електронні джерела.

Одночасно банк вживає відповідні запобіжні заходи, що спрямовані на:

- посилення ідентифікації клієнтів до встановлення ділових відносин з особами або компаніями цих країн;

- систематичне повідомлення про фінансові операції з клієнтами відповідних країн;

- попередження представників нефінансового сектору про те, що операції з фізичними або юридичними особами у відповідних країнах можуть містити ризик відмивання коштів, одержаних злочинним шляхом, або фінансування тероризму.

Особливої уваги потребує питання ідентифікації осіб, які пов'язані з політикою. Публічні діячі це – фізичні особи, які виконують або виконували визначені публічні функції в іноземних державах, а саме:

- глава держави, керівник уряду, міністри та їх заступники;

- депутати парламенту;

- члени верховного суду, конституційного суду або інших судових органів високого рівня, рішення яких не підлягають оскарженню, крім як за виняткових обставин;

- члени суду аудиторів або правлінь центральних банків;

- надзвичайні та повноважні посли, повірені у справах та високі посадовці збройних сил;

- члени адміністративних, управлінських чи наглядових органів державних підприємств, що мають стратегічне значення.

Ділові стосунки з особистостями, які займають високе положення в політиці, а також з особами або компаніями, які мають очевидне до них відношення, можуть наразити банк на значний юридичний ризик та/або вплинути на його репутацію. Завжди існує загроза того, що ці особи, особливо в країнах з розвинутою корупцією, зловживатимуть наданою їм владою для свого

власного збагачення протизаконним шляхом отримання хабара, розкрадання тощо.

Банк уточнює інформацію щодо ідентифікації та вивчення клієнта не рідше одного разу на рік, якщо ризик проведення клієнтом операцій з легалізації (відмивання) доходів, одержаних злочинним шляхом, оцінюється банком як великий. Для інших клієнтів термін уточнення інформації не повинен перевищувати трьох років. Обов'язкове уточнення інформації щодо ідентифікації та вивчення клієнта проводиться банком у разі:

а) зміни власника істотної участі;

б) зміни місцезнаходження (проживання) власника рахунку;

в) внесення змін до установчих документів;

г) закінчення строку дії наданих документів.

Банк поновлює відомості, отримані в результаті ідентифікації і вивчення клієнта, не рідше одного разу на рік у випадках, коли банк оцінює ризик як високий і не рідше ніж один раз у два роки в інших випадках.

В рамках ідентифікації клієнта банк проводить оцінювання фінансового стану клієнта.

Національний банк України (НБУ) рекомендує упровадити диференційований підхід до оцінювання фінансового стану клієнта:

- для клієнтів фізичних осіб (резидентів / нерезидентів);
- для клієнтів фізичних осіб підприємців;
- для клієнтів юридичних осіб (резидентів / нерезидентів).

Показниками для клієнтів – фізичних осіб (резидентів/нерезидентів) можуть бути:

- місце роботи (посада), сума доходу за основним місцем роботи, орієнтовний щомісячний сукупний дохід;
- наявність/відсутність нерухомого/рухомого майна;
- наявність цінних паперів, що знаходяться у власності (сума, кількість, емітент, динаміка котирування);
- сума депозитів в інших банках України (за кордоном);

- сума заборгованості по кредитах в інших банках.

Показниками для клієнтів – фізичних осіб-підприємців можуть бути:

- період діяльності з моменту державної реєстрації;

- наявність/відсутність працівників;

- орієнтовний щорічний прибуток/збиток (сума прибутку/збитку за попередній рік);

- здійснення клієнтом зовнішньоекономічної діяльності та її напряму (суми по договорах);

- термін дії договорів;

- країна (обслуговуючий банк);

- показники, визначені для фізичних осіб.

Показниками для клієнтів – юридичних осіб (резидентів/нерезидентів) такими показниками можуть бути;

- період діяльності з моменту державної реєстрації;

- наявність/відсутність філіальної мережі та дочірніх компаній (в тому числі за кордоном);

- орієнтовний щорічний дохід/збиток;

- сума депозитів в інших банках;

- наявність цінних паперів, що знаходяться у власності (вигляд коштовного паперу, сума, кількість, емітент, динаміка котирування);

- сума заборгованості по кредитах;

- наявність/відсутність поточних (в тому числі карткових) рахунків в інших банках;

- здійснення клієнтом зовнішньоекономічної діяльності та її напряму (зовнішньоекономічні договори, що діють: суми по договорах; термін дії договорів; країна; обслуговуючий банк), кількість штатних працівників.

Окрім того, НБУ рекомендує особливу увагу приділяти сумам і періодичності отримання коштів з вказаних клієнтом джерел, зокрема від кредитів, отриманих від банків, фінансової допомоги, відсотків від депозиту, перерахування з рахунків, відкритих в інших банках.

Національний банк України рекомендує, залежно від вигляду послуг, що банк надає клієнтам, отримувати фінансову звітність від окремих категорій клієнтів банку.

Фінансові банківські операції підлягають фінансовому моніторингу. Відповідно до Базового Закону, фінансова операція – це будь-які дії щодо активів, здійснені за допомогою суб'єкта первинного фінансового моніторингу.

Фінансова операція підлягає обов'язковому фінансовому моніторингу у разі, якщо сума, на яку вона проводиться, дорівнює чи перевищує 150 тис. гривень або дорівнює чи перевищує суму в іноземній валюті, еквівалентній 150 тис. гривень, та має одну або більше таких ознак:

- переказ грошових коштів на анонімний (номерний) рахунок за кордон і надходження грошових коштів з анонімного (номерного) рахунку з-за кордону, а також переказ коштів на рахунок, відкритий у фінансовій установі в країні, що віднесена Кабінетом Міністрів України до переліку офшорних зон;

- купівля-продаж чеків, дорожніх чеків або інших подібних платіжних засобів за готівку;

- зарахування або переказ коштів, надання або отримання кредиту (позики), проведення інших фінансових операцій у разі, якщо хоча б одна з сторін – учасників фінансової операції є фізичною або юридичною особою, що має відповідну реєстрацію, місце проживання чи місцезнаходження в країні (на території), що не виконують чи неналежним чином виконують рекомендації міжнародних, міжурядових організацій, що здійснюють діяльність у сфері боротьби з легалізацією (відмиванням) доходів, одержаних злочинним шляхом, або фінансуванням тероризму, або однією зі сторін є особа, яка має рахунок у банку, зареєстрованому у вищезазначеній країні (території). Перелік таких країн (територій) визначається відповідно до порядку, встановленого Кабінетом Міністрів України, на основі висновків міжнародних, міжурядових організацій, діяльність яких спрямована на протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму, і підлягає опублікуванню;

- фінансові операції з готівкою (внесення, переказ, отримання коштів);

- здійснення розрахунку за фінансову операцію у готівковій формі;

- зарахування коштів на поточний рахунок юридичної або фізичної особи-підприємця чи списання коштів з поточного рахунка юридичної або фізичної особи-підприємця, період діяльності якої не перевищує трьох місяців з дня реєстрації, або зарахування коштів на поточний рахунок чи списання готівки з поточного рахунка юридичної або фізичної особи-підприємця у разі, якщо операції на зазначеному рахунку не здійснювалися з дня його відкриття;

- переказ коштів за кордон за зовнішньоекономічними договорами (контрактами), крім переказів коштів за договорами (контрактами), що передбачають фактичне постачання товарів на митну територію України;

- обмін банкнот, особливо іноземної валюти, на банкноти іншого номіналу;

- здійснення фінансових операцій з цінними паперами на пред'явника, не депонованими в депозитарних установах;

- проведення фінансових операцій з векселями (крім фінансових казначейських векселів), ордерними цінними паперами;

- здійснення розрахунку за фінансовою операцією у готівковій формі;

- та інше, відповідно до ст.15 Базового Закону.

Фінансова операція підлягає внутрішньому фінансовому моніторингу, якщо у суб'єкта фінансового моніторингу виникають підозри, що ґрунтуються, зокрема, на:

- критеріях ризиків, визначених самостійно суб'єктом фінансового моніторингу з урахуванням критеріїв ризиків, встановлених ДСФМ;

- встановлені за результатами проведеного аналізу фактів (факту) невідповідності фінансових операцій фінансовому стану та/або змісту діяльності клієнта;

- типологічних досліджень у сфері фінансового моніторингу.

У разі якщо у банку виникають підстави вважати, що фінансова операція пов'язана з легалізацією (відмиванням) доходів, одержаних злочинним шляхом, або фінансуванням тероризму, внутрішній фінансовий моніторинг проводиться

також щодо інших фінансових операцій, в уточненні яких виникла необхідність.

Також, внутрішньому фінансовому моніторингу підлягають операції відповідно до типології міжнародних організацій, що здійснюють діяльність у сфері протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму.

Під час розробки програми виявлення в діяльності клієнтів операцій, що підлягають обов'язковому контролю, й інших операцій з грошовими коштами або іншим майном, пов'язаних з легалізацією (відмиванням) грошей, отриманих злочинним шляхом, банк визначає для себе критерії виявлення та ознаки сумнівних операцій згідно діючого законодавства.

Уповноважений по контролю за дотриманням законодавства приймає рішення про необхідність реєстрації операції, що підлягає фінансовому моніторингу. Остаточне рішення щодо віднесення такої операції до операцій, що підлягали обов'язковому, внутрішньому фінансовому моніторингу, або призначалися для фінансування терористичної діяльності, її реєстрації та інформування ДСФМУ.

Зареєстровані та затверджені фінансові операції заносяться співробітниками Відділу фінансового моніторингу до електронного реєстру і надсилаються до Уповноваженого органу у формі файлів-повідомлень.

Реєстрація фінансових операцій, що підлягають фінансовому моніторингу, здійснюється у відповідному реєстрі, який формується та ведеться банком (філією) і є електронним документом визначеної структури. Формат і структура реєстру та порядок реєстрації фінансових операцій у реєстрі визначаються відповідальним працівником банку (філії).

Реєстр фінансових операцій, що підлягають фінансовому моніторингу, є документом з обмеженим доступом. Порядок та режим доступу працівників банку до реєстру встановлюються відповідальним працівником банку (філії). Відповідальний працівник банку (філії) несе особисту відповідальність за

захист реєстру від знищення, несанкціонованого доступу, модифікації або викривлення даних.

Для реєстрації фінансової операції, що підлягає фінансовому моніторингу, до реєстру вносяться такі дані, пов'язані з цією операцією:

а) порядковий номер реєстрації фінансової операції в реєстрі з початку календарного року;

б) унікальний номер операції в системі автоматизації банку (за його наявності);

в) дата надходження розрахункових або інших документів, що є підставою для здійснення операції;

г) сума операції у валюті її проведення та її еквівалент у національній валюті за офіційним курсом гривні до іноземної валюти, установленим Національним банком України на день проведення операції;

ґ) прізвище, ім'я, по-батькові фізичної особи або назва юридичної особи, що здійснює операцію, та ідентифікаційний номер (код) цієї особи;

д) прізвище, ім'я, по-батькові фізичної особи або назва юридичної особи-контрагента (за його наявності);

е) вид операції;

є) назва, номер і дата первинного документа, на підставі якого здійснюється операція;

ж) ознака (ознаки) операції, за якою вона підлягає фінансовому моніторингу;

з) прізвище та ініціали працівника, який повідомив про цю операцію;

и) прізвище та ініціали працівника, який вніс інформацію про цю операцію до реєстру.

Перелік реквізитів для надсилання банком (філією) уповноваженому органу повідомлення про фінансову операцію, що підлягає фінансовому моніторингу, та осіб, які її здійснюють (здійснили), представлені в таблиці 2.9.

Таблиця 2.9

Перелік реквізитів для надсилання банком (філією) уповноваженому органу повідомлення про фінансову операцію, що підлягає фінансовому моніторингу

Необхідні дані	
1. Дані про банк (філію), що надає інформацію	1) назва згідно з реєстрацією; 2) МФО; 3) ідентифікаційний код згідно з Єдиним державним реєстром підприємств та організацій України; 4) місцезнаходження; 5) номер телефону.
2. Дані про відповідального працівника банку (філії)	1) посада; 2) прізвище, ім'я, по-батькові; 3) номер телефону; 4) адреса електронної пошти.
3. Дані про операцію	1) унікальний номер операції в системі автоматизації банку (за його наявності); 2) порядковий номер реєстрації фінансової операції в реєстрі; 3) ознака здійснення операції; 4) дата та час здійснення (відмови в здійсненні) операції; 5) код валюти операції або код банківського металу; 6) сума операції у валюті її проведення та її еквівалент у національній валюті за офіційним курсом гривні до іноземної валюти, установленим Національним банком України на день проведення операції; 7) код (коди) ознаки (ознак) фінансової операції, що підлягає фінансовому моніторингу; 8) код виду операції; 9) призначення платежу; 10) пов'язані операції (за наявності відповідної інформації); 11) коментар.
4. Дані про клієнта	
для юридичної особи	1) повна та скорочена назва; 2) ознака резидентності; 3) країна реєстрації; 4) ідентифікаційний код згідно з Єдиним державним реєстром підприємств та організацій України; 5) юридична номер рахунка клієнта, що використовується для здійснення операції; адреса.
4. Дані про клієнта	
для фізичної особи:	1) тип (фізична особа, фізична особа-суб'єкт підприємницької діяльності); 2) прізвище, ім'я, по-батькові; 3) ознака резидентності; 4) країна; 5) ідентифікаційний номер згідно з Державним реєстром фізичних осіб-платників податків та інших обов'язкових платежів; 6) місце проживання або тимчасового перебування (поштова адреса); 7) дані про документ, що згідно з законодавством України засвідчує особу (назва, серія та номер документа, дата видачі

Необхідні дані	
	документа, повна назва органу, що видав документ); 8) номер рахунка клієнта, що використовується для здійснення операції (у разі його наявності).
5. Дані про особу, яка діє від імені клієнта	
для юридичної особи	1) повна або скорочена назва; 2) ідентифікаційний код згідно з Єдиним державним реєстром підприємств та організацій України; 3) юридична адреса; 4) дані про документ, що дає право діяти від імені клієнта.
для фізичної особи:	1) прізвище, ім'я, по-батькові; 2) ідентифікаційний номер згідно з Державним реєстром фізичних осіб-платників податків та інших обов'язкових платежів; 3) місце проживання або тимчасового перебування (поштова адреса); 4) дані про документ, що згідно з законодавством України засвідчує особу (назва, серія та номер документа, дата видачі документа, повна назва органу, що видав документ); 5) дані про документ, що дає право діяти від імені клієнта.
6. Інші учасники операції (за їх наявності) та дані про них	1) вид участі в операції (контрагент, представник контрагента, фактичний вигодоодержувач тощо); 2) для юридичної особи – повна або скорочена назва; 3) для фізичної особи – прізвище, ім'я, по-батькові; 4) інша інформація про учасника (у разі її наявності).
для юридичної особи	1) ознака резидентності; 2) країна реєстрації; 3) ідентифікаційний код згідно з Єдиним державним реєстром підприємств та організацій України; 4) юридична адреса; 5) номер рахунка учасника, що використовується для здійснення операції; дані про банк (філію), у якому відкритий рахунок, що використовується для здійснення операції: назва, МФО – для резидента або BIC – для нерезидента, юридична адреса.
для фізичної особи	1) тип учасника (фізична особа, фізична особа-суб'єкт підприємницької діяльності); 2) ознака резидентності; 3) країна громадянства; 4) ідентифікаційний номер згідно з Державним реєстром фізичних осіб-платників податків та інших обов'язкових платежів; 5) місце проживання або тимчасового перебування (поштова адреса); 6) номер рахунка учасника, що використовується для здійснення операції; 7) дані про банк (філію), у якому відкритий рахунок, що використовується для здійснення операції: назва, МФО – для резидента або BIC – для нерезидента, юридична адреса; 8) інша інформація.
7. Дані про коррахунок, що використовується для здійснення операції в іноземній валюті (у разі наявності)	1) номер рахунка; 2) назва; 3) МФО – для резидента або BIC – для нерезидента; 4) юридична адреса фінансової установи.

Банки повинні зберігати не менше п’яти років всі необхідні записи з трансакцій, що проводились у країні або за кордоном для того, щоб вони могли швидко давати відповіді на запити інформації компетентних органів влади. Такі документи повинні бути достатніми для того, щоб дозволити реконструкцію окремих трансакцій (включаючи суми та типи валют, що використовувались) для того, щоб забезпечити, при необхідності, свідчення для судового переслідування кримінальної поведінки. Також, банки повинні зберігати документи з ідентифікації клієнта (наприклад, копії або записи офіційних ідентифікаційних документів, таких, як паспорти, посвідчення особи, права на автомобіль або подібні документи), файли рахунків і ділової кореспонденції не менше як за останні п’ять років після того, як рахунок закрито. Ці документи мають бути доступними для місцевих компетентних органів влади у контексті відповідних кримінальних переслідувань і в розслідуваннях.

Інформація про банки чи клієнтів, що збирається під час проведення банківського нагляду, становить банківську таємницю. Інформація про банки чи клієнтів, отримана Національним банком України відповідно до міжнародного договору або за принципом взаємності від органу банківського нагляду іншої держави для використання з метою банківського нагляду або запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом, чи фінансуванню тероризму, становить банківську таємницю.

Банківська таємниця – це інформація щодо діяльності та фінансового стану клієнта, що стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку (ст. 60 Закону України «Про банки та банківську діяльність»).

Банківською таємницею, зокрема, є:

1) відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;

2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди;

3) фінансово-економічний стан клієнтів;

4) системи охорони банку та клієнтів;

5) інформація про організаційно-правову структуру юридичної особи-клієнта, її керівників, напрями діяльності;

6) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;

7) інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;

8) коди, що використовуються банками для захисту інформації.

Вищезазначене не поширюється на інформацію, що підлягає опублікуванню. Перелік інформації, що підлягає обов'язковому опублікуванню, встановлюється Національним банком України та додатково самим банком на його розсуд.

Банки зобов'язані забезпечити збереження банківської таємниці шляхом:

1) обмеження кола осіб, які мають доступ до інформації, що становить банківську таємницю;

2) організації спеціального діловодства з документами, що містять банківську таємницю;

3) застосування технічних засобів для запобігання несанкціонованому доступу до електронних та інших носіїв інформації;

4) застосування застережень щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком і клієнтом.

Службовці банку при вступі на посаду підписують зобов'язання щодо збереження банківської таємниці. Керівники та службовці банків зобов'язані не розголошувати та не використовувати з вигодою для себе чи для третіх осіб конфіденційну інформацію, що стала відома їм при виконанні своїх службових обов'язків.

Банк має право надавати інформацію, що містить банківську таємницю, приватним особам та організаціям для забезпечення виконання ними своїх функцій або надання послуг банку відповідно до укладених між такими

особами (організаціями) та банком договорів, у тому числі про відступлення права вимоги до клієнта, за умови, що передбачені договорами функції та/або послуги стосуються діяльності банку, яку він здійснює відповідно до статті 47 цього Закону.

Приватні особи та організації, які при виконанні своїх функцій або наданні послуг банку безпосередньо чи опосередковано отримали конфіденційну інформацію, зобов'язані не розголошувати цю інформацію і не використовувати її на свою користь чи на користь третіх осіб.

У разі заподіяння банку чи його клієнту збитків шляхом витоку інформації про банки та їх клієнтів з органів, які уповноважені здійснювати банківський нагляд, збитки відшкодовуються винними органами.

Згідно Закону України «Про Національну поліцію» (стаття 11 п. 17), поліції для виконання покладених на неї обов'язків надається право: одержувати безперешкодно та безплатно від підприємств, установ і організацій незалежно від форм власності та об'єднань громадян на письмовий запит відомості (в тому числі й ті, що становлять комерційну та банківську таємницю), необхідні у справах про злочини, що знаходяться у провадженні міліції. Отримання від банків інформації, що містить банківську таємницю, здійснюється у порядку та обсязі, встановлених Законом України «Про банки і банківську діяльність».

Згідно Закону України «Про службу безпеки України» (стаття 25), Службі безпеки України, її органам і співробітникам для виконання покладених на них обов'язків надається право:

одержувати на письмовий запит керівника відповідного органу Служби безпеки України від міністерств, державних комітетів, інших відомств, підприємств, установ, організацій, військових частин, громадян та їх об'єднань дані й відомості, необхідні для забезпечення державної безпеки України, а також користуватись з цією метою службовою документацією і звітністю. Отримання від банків інформації, яка містить банківську таємницю, здійснюється у порядку та обсязі, встановлених законом України «Про банки і

банківську діяльність», а саме інформація щодо юридичних та фізичних осіб, яка містить банківську таємницю, розкривається банками:

1) на письмовий запит або з письмового дозволу власника такої інформації;

2) за рішенням суду;

3) органам прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України, Антимонопольного комітету України – на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи-суб'єкта підприємницької діяльності за конкретний проміжок часу;

4) органам Державної фіскальної служби України на їх письмову вимогу щодо наявності банківських рахунків;

5) центральному органу виконавчої влади зі спеціальним статусом з питань фінансового моніторингу на його запит щодо фінансових операцій, пов'язаних з фінансовими операціями, що стали об'єктом фінансового моніторингу (аналізу) згідно з законодавством щодо запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму, а також учасників зазначених операцій;

6) органам державної виконавчої служби на їх письмову вимогу з питань виконання рішень судів та рішень, що підлягають примусовому виконанню відповідно до Закону України «Про виконавче провадження», стосовно стану рахунків конкретної юридичної особи або фізичної особи, фізичної особи-суб'єкта підприємницької діяльності.

Обмеження стосовно отримання інформації, що містить банківську таємницю, передбачені цією статтею, не поширюються на службовців Національного банку України або уповноважених ними осіб, які в межах повноважень, наданих Законом України «Про Національний банк України», здійснюють функції банківського нагляду або валютного контролю.

Національний банк України відповідно до міжнародного договору України або за принципом взаємності має право надавати інформацію, отриману при

здійсненні нагляду за діяльністю банків, органу банківського нагляду іншої держави, а також отримувати від органу банківського нагляду іншої держави таку інформацію. Надана (отримана) інформація може бути використана виключно з метою банківського нагляду або запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом, чи фінансуванню тероризму.

Положення частин другої та четвертої цієї статті не поширюються на випадки надання спеціально уповноваженому органу виконавчої влади з питань фінансового моніторингу інформації про фінансові операції у випадках, передбачених законом, та органам державної податкової служби - інформації про відкриття (закриття) рахунків платників податків відповідно до статті 69 Податкового кодексу України. А саме: банки та інші фінансові установи зобов'язані надіслати повідомлення про відкриття або закриття рахунка платника податків – юридичної особи, у тому числі відкритого через його відокремлені підрозділи, чи самозайнятої фізичної особи до органу державної податкової служби, в якому обліковується платник податків, протягом трьох робочих днів з дня відкриття/закриття рахунка (включаючи день відкриття/закриття).

Постановою Національного банку України від 16.11.2000 р. №451 «Про затвердження Правил надання банками на письмову вимогу керівників відповідних спеціальних підрозділів по боротьбі з організованою злочинністю інформації і документів» НБУ зобов'язав комерційні банки неухильно виконувати письмові вимоги керівників відповідних спецпідрозділів МВС і СБУ по боротьбі з організованою злочинністю щодо надання інформації і документів про операції, рахунки, вклади фізичних осіб, за якими провадяться справи органами служби безпеки, внутрішніх справ, і юридичних осіб.

Згідно статті 32 Закону України «Про інформацію», під інформаційним запитом щодо доступу до офіційних документів розуміється звернення з вимогою про надання можливості ознайомлення з офіційними документами.

Запит може бути індивідуальним або колективним. Він подається у письмовій формі.

Вимога відповідного державного органу на отримання інформації, яка містить банківську таємницю, повинна:

1) бути викладена на бланку державного органу встановленої форми;

2) бути надана за підписом керівника державного органу (чи його заступника), скріпленого гербовою печаткою;

3) містити передбачені цим Законом підстави для отримання цієї інформації;

4) містити посилання на норми закону, відповідно до яких державний орган має право на отримання такої інформації.

Банку забороняється надавати інформацію про клієнтів іншого банку, навіть якщо їх імена зазначені у документах, угодах та операціях клієнта.

Банк має право надавати інформацію, що становить банківську таємницю, іншим банкам та Національному банку України в обсягах, необхідних при наданні кредитів, банківських гарантій.

Банк має право розкривати інформацію, що містить банківську таємницю, особі (в тому числі, яка уповноважена діяти від імені держави), на користь якої відчужуються активи та зобов’язання банку при виконанні заходів, передбачених програмою фінансового оздоровлення банку, або під час здійснення процедури ліквідації. Національний банк України (тимчасовий адміністратор) має право надавати Міністерству фінансів України інформацію, яка містить банківську таємницю щодо банків, участь у капіталізації яких бере держава.

Термін вивчення запиту на предмет можливості його задоволення не повинен перевищувати десяти календарних днів. Протягом вказаного терміну державна установа письмово доводить до відома запитувача, що його запит буде задоволено або що запитуваний документ не підлягає наданню для ознайомлення. Задоволення запиту здійснюється протягом місяця, якщо інше

не передбачено законом. Аналогічний термін розгляду встановлюється і щодо запиту про надання письмової інформації.

Відмова в задоволенні запиту доводиться до відома запитувача у письмовій формі з роз'ясненням порядку оскарження прийнятого рішення.

У відмові має бути зазначено:

1) посадову особу державної установи, яка відмовляє у задоволенні запиту;

2) дату відмови;

3) мотивовану підставу відмови.

Відстрочка задоволення запиту допускається в разі, якщо запитуваний документ не може бути надано для ознайомлення у місячний термін. Повідомлення про відстрочку доводиться до відома запитувача у письмовій формі з роз'ясненням порядку оскарження прийнятого рішення.

У повідомленні про відстрочку має бути зазначено:

1) посадову особу державної установи, яка відмовляє у задоволенні запиту у визначений місячний термін;

2) дату надсилання або видачі повідомлення про відстрочку;

3) причини, з яких запитуваний документ не може бути видано у встановлений законодавством термін;

4) термін, у який буде задоволено запит.

Не підлягають обов'язковому наданню для ознайомлення за інформаційними запитами офіційні документи, що містять у собі:

- інформацію, визнану у встановленому порядку державною таємницею;

- конфіденційну інформацію;

- інформацію про оперативну та слідчу роботу органів прокуратури, МВС, СБУ, роботу органів дізнання та суду у тих випадках, коли її розголошення може зашкодити оперативним заходам, розслідуванню чи дізнанню, порушити право людини на справедливий та об'єктивний судовий розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи;

- інформацію, що стосується особистого життя громадян, документи, що становлять внутрівідомчу службову кореспонденцію (доповідні записки,

переписка між підрозділами та інше), якщо вони пов'язані з розробкою напряму діяльності установи, процесом прийняття рішень і передують їх прийняттю;

- інформацію, що не підлягає розголошенню згідно з іншими законодавчими або нормативними актами. Установа, до якої звернуто запит, може не надавати для ознайомлення документ, якщо він містить інформацію, що не підлягає розголошенню на підставі нормативного акта іншої державної установи, а та державна установа, яка розглядає запит, не має права вирішувати питання щодо її розсекречення;

- інформацію фінансових установ, що підготовлена для контролюючих органів, крім випадків, коли така інформація вимагається за письмовим запитом контролюючого органу для здійснення податкового, митного, бюджетного та валютного контролю.

Особи, які винні в порушенні порядку розкриття та використання банківської таємниці, несуть відповідальність згідно з законами України.

Приватні особи та організації, які при виконанні своїх функцій або наданні послуг банку безпосередньо чи опосередковано отримали конфіденційну інформацію, зобов'язані не розголошувати цю інформацію та не використовувати її на свою користь чи на користь третіх осіб.

У разі заподіяння банку чи його клієнту збитків шляхом витоку інформації про банки та їх клієнтів з органів, які уповноважені здійснювати банківський нагляд, збитки відшкодовуються винними органами.

Розглянувши порядок зберігання інформації, поняття комерційної та банківської таємниці, умови та порядок її розкриття, а також нормативно-правову базу щодо організації системи фінансового моніторингу, порядок проведення ідентифікації клієнтів, оцінювання їх фінансового стану та періодичність їх здійснення, порядок виявлення фінансових операцій, їх класифікацію та реєстрацію зазначимо, що проблематика організації фінансового моніторингу в комерційних банках є актуальною та потребує глибшого опрацювання з огляду на її важливість для фінансово-кредитних

організацій. Комерційні банки функціонують в умовах невизначеності, ризиковості, що зумовлює необхідність не лише комплексного запровадження заходів фінансового моніторингу на рівні як окремої банківської установи, так й загалом вітчизняної фінансово-кредитної системи, а й постійного перегляду його методичних аспектів з метою удосконалення та підвищення ефективності.

Список використаних джерел:

1. *Фінансовий моніторинг в банку: навчальний посібник/ Дмитров С.О.; Коваленко В.В.; Єжов А.В.; Бережний О.М.- Суми: ВТД "Університетська книга", 2008.- 336 с.*
2. *Дмитров С. О. Управління фінансовою безпекою комерційного банку / О. С. Дмитров //Фінансовий простір. – № 2 (6). – 2012. – С. 11 – 15.*
3. *Дмитров С.О., Медвідь Т.А. Новітня компонента в системі банківських ризиків / Сергій Дмитров, Тетяна Медвідь // Науково-практичний журнал Вісник Національного банку України. — 2010. — №4 (170). — С. 11-14.*

РОЗДІЛ 3
РОЛЬ КАДРОВОЇ БЕЗПЕКИ У РЕАЛІЗАЦІЇ МЕХАНІЗМУ ПРОТИДІЇ ЕКОНОМІЧНИМ ЗЛОЧИНАМ

3.1. ОРГАНІЗАЦІЯ НЕЗАЛЕЖНОГО ЗОВНІШНЬОГО АУДИТУ ПІДСИСТЕМИ ОРГАНІЗАЦІЇ БЕЗПЕКИ ПРАЦІ НА БУДІВЕЛЬНИХ ПІДПРИЄМСТВАХ З ПОЗИЦІЙ ЕКОНОМІЧНОЇ БЕЗПЕКИ

АНДРІЄНКО ВАСИЛЬ МИКОЛАЙОВИЧ*, д.е.н., доцент,*
професор кафедри менеджменту та економічної безпеки,
АНДРІЄНКО МИКОЛА ВАСИЛЬОВИЧ*, д.е.н., доцент,*
професор кафедри менеджменту та економічної безпеки,
Черкаського національного університету ім. Богдана Хмельницького

Аналіз закордонного досвіду в галузі менеджменту охорони праці свідчить, що його регулювання необхідно здійснювати на підставі оцінки ризиків виникнення нещасних випадків та аварій на виробництві у відповідності зі Стандартом серії OHSAS 18001 «Система менеджменту охорони здоров’я та безпеки персоналу», який не має статусу міжнародного стандарту ISO, але широко використовується у всьому світі і вважається одним із самих досконалих стандартів по організації менеджменту з питань охорони праці. В ньому система менеджменту управління охороною праці будується на ідентифікації та оцінці загроз виникнення нещасних випадків на виробництві та професійних захворювань.

Зазначеним стандартом серії OHSAS 18001 «Система менеджменту охорони здоров’я та безпеки персоналу» передбачене проведення незалежного зовнішнього аудиту системи управління безпекою праці, проте, сам механізм такого аудиту чітко не встановлений.

Законодавство України також передбачає можливість залучення зовнішніх незалежних експертів-аудиторів для здійснення перевірки стану системи управління охороною праці на підприємствах. Але, оскільки питання безпеки праці є більш широкими та включають в себе й інші питання поряд з питаннями охорони праці, а також безпосередньо впливають на стан системи економічної безпеки всіх підприємств, в тому числі й будівельної галузі, пропонуємо авторський підхід до проведення незалежного зовнішнього аудиту системи управління безпекою праці як складової системи економічної безпеки

будівельних підприємств.

Під поняттям «*незалежний зовнішній аудит підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємст*в» пропонуємо розуміти документально оформлений системний незалежний процес діагностики стану відповідної підсистеми, який здійснюється аудиторською організацією на замовлення власника будівельного підприємства (Додаток С).

Метою проведення незалежного зовнішнього аудиту є діагностика стану підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємств [259].

Основними завданнями аудиту є:

- збір достовірної інформації про об'єкт аудиту та формування на її основі аудиторського висновку;
- встановлення відповідності об'єкта аудиту вимогам законодавства з питань безпеки праці;
- оцінка впливу діяльності об'єкта аудиту на стан системи управління безпекою праці;
- оцінка ефективності, повноти і обґрунтованості заходів, що вживаються для забезпечення безпеки праці на об'єкті аудиту [54].

Конкретні завдання аудиту в кожному окремому випадку визначаються замовником, виходячи з його потреб та характеру діяльності об'єкта аудиту.

Основними напрямами незалежного зовнішнього аудиту підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємств є наступні:

- професійний добір для працівників, які виконують роботи підвищеної небезпеки, з урахуванням стану здоров’я та психофізіологічних показників;
- навчання та пропаганда знань з охорони праці;
- безпечний стан обладнання;
- безпечний стан виробничих процесів;
- безпечний стан будівель та споруд;

- забезпечення нормативних санітарно-гігієнічних умов праці;
- наявність засобів індивідуального захисту;
- оптимальні режими праці та відпочинку;
- лікувально–профілактичне обслуговування працюючих;
- санітарно–побутове обслуговування.

Основними функціями незалежного зовнішнього аудиту підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємств є:

- *контролююча* – передбачає перевірку всіх напрямів забезпечення безпеки праці на підприємствах на їх відповідність законодавчо встановленим нормам;
- *консультаційна* – надає поради щодо приведення у відповідність всіх напрямів забезпечення безпеки праці у відповідність із законодавчо встановленими нормами;
- *запобіжна* – дозволяє виявити та виправити недоліки у стані системи управління безпекою праці на підприємстві до перевірки контролюючими органами.

Незалежному зовнішньому аудиту підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємств притаманні такі *характерні риси*:

- добровільність;
- незалежність;
- документальне оформлення результатів;
- засвідчення стану відповідності вимогам законів та інших нормативно-правових актів з питань безпеки праці.

Основними принципами незалежного зовнішнього аудиту є незалежність, законність, обґрунтованість, об'єктивність, неупередженість, достовірність, документованість, професійна компетентність, персональна (індивідуальна) відповідальність виконавця аудиту при проведенні аудиту та складанні аудиторського висновку.

Основними суб'єктами незалежного зовнішнього аудиту підсистеми

організації безпеки праці як складової системи економічної безпеки будівельних підприємств є: замовник та виконавець (рис. 3.1).

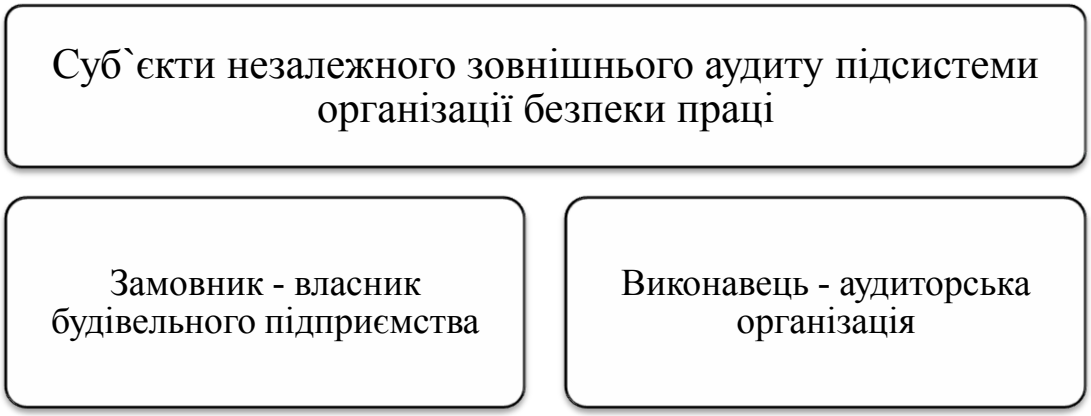


Рис. 3.1. Суб’єкти незалежного зовнішнього аудиту підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємств

Складено особисто автором [54]

Замовником незалежного зовнішнього аудиту є власник чи власники будівельного підприємства, які мають права та обов’язки (табл. 3.1)

Таблиця 3.1

Права та обов’язки замовника незалежного зовнішнього аудиту

Права	Обов’язки
вільно визначати виконавців аудиту, давати аудиторській організації завдання на проведення аудиту, отримувати інформацію про хід аудиту, одержувати та використовувати висновки та свідоцтва з проведення аудиту	забезпечувати фінансування проведення аудиту, своєчасне приймання та оплату виконаних робіт та наданих послуг
право на відшкодування збитків, заподіяних неправомірними діями аудиторської організації під час проведення аудиту	надавати аудиторській організації всю наявну в нього інформацію, письмові чи усні пояснення щодо об'єктів аудиту
інші права відповідно до законодавства України	не допускати дій, спрямованих на примушування виконавця аудиту до зміни форм і методів роботи чи висновків аудиту
	забезпечувати доступ виконавців аудиту на об'єкт, сприяти їм у проведенні дій, необхідних для належного виконання покладених на них завдань
	виконувати інші дії, пов'язані з проведенням аудиту відповідно до законодавства України

Складено особисто автором [259]

Виконавцем незалежного зовнішнього аудиту є *аудиторська організація*, під якою пропонуємо розуміти суб'єкт господарської діяльності, який здійснює аудит стану підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємств та акредитована відповідно до вимог чинного законодавства. У складі аудиторської організації працюють незалежні аудитори – фізичні особи, які пройшли у встановленому порядку навчання та отримали документ на право здійснення аудиту стану системи управління безпекою праці.

На нашу думку, аудиторська організація, повинна відповідати наступним критеріям:

- бути юридичною особою – резидентом України;
- мати в своєму штаті аудиторів з систем управління якістю;
- мати в своєму штаті аудиторів з систем управління безпекою праці та охорони здоров'я, не менше 2-х фахівців;
- мати в своєму штаті експертів технічних з промислової безпеки, які працюють на постійних засадах з кожного заявленого напрямку експертної діяльності, з кожного заявленого виду устаткування;
- мати в своєму штаті фахівців з оцінки умов праці на робочих місцях;
- мати атестат акредитації Національного органа з акредитації як органу, що здійснює інспектування згідно з ДСТУ ISO/IEC 17020;
- мати сертифікат на систему управління якістю згідно з ДСТУ ISO 9001;
- мати актуалізований фонд нормативно-правових актів та нормативних документів та систему його актуалізації;
- мати необхідне інформаційно-технічне забезпечення робіт з ведення обліку даних про проведені роботи.

Для виконання перевірок як аудитори можуть бути допущені спеціалісти, які пройшли належну підготовку (навчання) і практично взяли участь у двох перевірках як стажери.Обсяг підготовки повинен бути таким, щоб забезпечити компетентність аудитора як у питаннях безпеки праці на підприємстві, так і в правилах проведення перевірок, зокрема:

- знання нормативно-правових вимог з безпеки праці, на відповідність яким здійснюються перевірки;

- методи і техніка огляду, опитування, оцінювання та підготовки звітів;

- додаткові навики, необхідні для проведення перевірок, такі, як спілкування, документування, здібність до керування, вміння планувати й аналізувати.

На нашу думку, аудитор повинен:

- мати достатньо широкий світогляд;

- бути витриманим;

- володіти логічним мисленням і твердістю волі;

- вміти реально оцінювати ситуацію;

- розуміти роль підрозділів, їх діяльності та виконуваних процесів.

Ці якості необхідні аудитору для того, щоб:

- неупереджено збирати факти й оцінювати об'єктивні докази;

- зберігати вірність цілям перевірки без побоювання або упередження;

- постійно оцінювати результати перевірки;

- будувати свої відносини з опитуваним персоналом так, щоб най кращим чином сприяти досягненню цілей перевірки;

- здійснювати процес перевірки, не відволікаючись на другорядне;

- присвячувати всю увагу перевірці й надавати підтримку процесу перевірки;

- реагувати швидко й адекватно у конфліктних ситуаціях;

- робити об'єктивні висновки на підставі проведених спостережень;

- зберігати твердість висновку, незважаючи на спроби тиску внести зміни, не обґрунтовані доказами.

Національний орган з акредитації здійснює акредитацію аудиторських організацій шляхом надання атестату акредитації встановленого зразка згідно з вимогами Закону України „Про акредитацію органів з оцінки відповідності” з урахуванням зазначених вище вимог.

Пропонуємо забороняти здійснення незалежного зовнішнього аудиту будівельних підприємств тим аудиторам, які мають акції цих об'єктів або у іншій формі мають безпосереднє відношення до них. Аудиторська організація під час проведення аудиту має певні права та обов’язки (табл. 3.2).

Таблиця 3.2

Права та обов’язки аудиторської організації

Права	Обов’язки
самостійно визначати форми і методи проведення аудиту відповідно до законодавства та договору із замовником аудиту	повідомляти замовника про всі виявлені у процесі проведення аудиту випадки порушення законодавства про промислову безпеку і охорону праці, стандартів, норм, правил та відображати цю інформацію у висновку про проведення аудиту
отримувати документи, матеріали та інші відомості, наявні у замовника об'єкта аудиту, необхідні для проведення аудиту	невідкладно інформувати про виявлену у процесі проведення аудиту загрозу аварійної ситуації керівника (власника) об'єкта аудиту
залучати на договірних засадах для вирішення окремих питань, що виникають у процесі проведення аудиту і вимагають спеціальних знань, фахівців відповідного профілю, не покладаючи на них відповідальність за висновки аудиту	забезпечувати належне збереження та своєчасне повернення документів, які одержані від власника об'єкта аудиту, замовника та інших осіб для проведення аудиту
	невідкладно інформувати замовника про відомі аудиторській організації причини, що унеможливлюють проведення чи продовження аудиту
	заявляти самовідвід за наявності особистої зацікавленості у результатах аудиту
	дотримуватися встановлених законодавством та договором на проведення аудиту вимог щодо конфіденційності інформації, яка отримана або стала йому відома під час виконання цієї роботи

Складено особисто автором

Основними об'єктами незалежного зовнішнього аудиту підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємств є:

- підприємства, установи та організації, їх філії та представництва чи об'єднання, окремі виробництва, інші суб’єкти господарювання;
- системи управління охороною праці та промисловою безпекою;
- роботи підвищеної небезпеки.

Проведення незалежного зовнішнього аудиту стану підсистеми організації

безпеки праці як складової системи економічної безпеки будівельних підприємств пропонуємо здійснювати згідно з рис. 3.2.

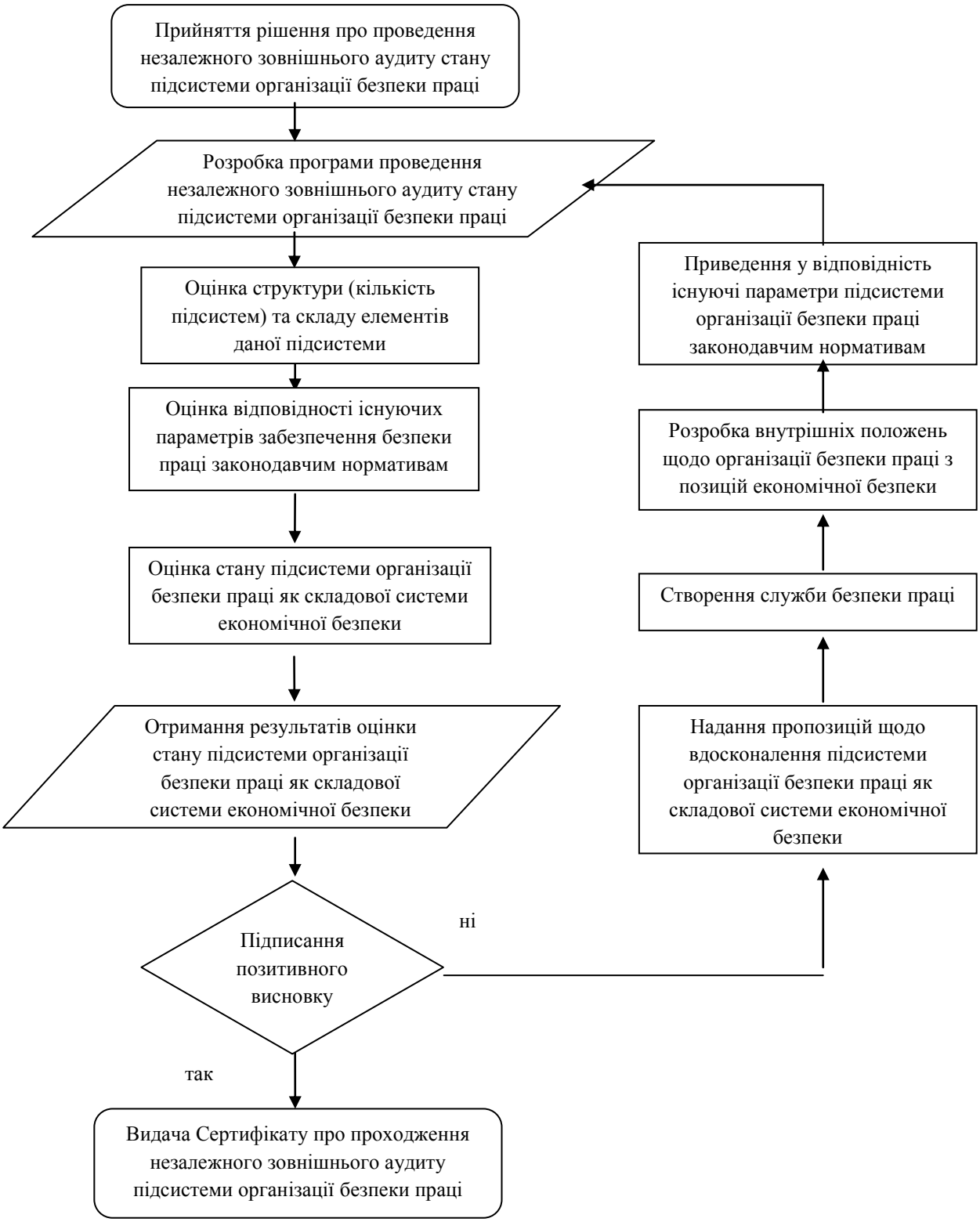


Рис. 3.2. Алгоритм проведення незалежного зовнішнього аудиту стану підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємств

Складено особисто автором

Аудит проводиться на підставі договору між замовником та виконавцем, укладеному відповідно до вимог законодавства України, згідно з яким аудиторська організація несе визначену законом та договором відповідальність перед замовником за виконання визначених договором зобов'язань та достовірність висновків аудиту.

Відносини у сфері незалежного зовнішнього аудиту стану підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємств регулюються Конституцією України, Законом України „Про охорону праці”, Законом України „Про дозвільну систему у сфері господарської діяльності”, Законом України „Про акредитацію органів з оцінки відповідності”, іншими актами законодавства України.

Аудиторська організація розробляє Програму аудиту та погоджує її з замовником. Дана програма має містити основні об’єкти аудиту та терміни їх перевірки [260].

На нашу думку, перевірку об’єктів аудиту доцільно здійснювати в розрізі підсистем другого рівня підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємств та в розрізі функціональних складових системи економічної безпеки будівельних підприємств, зазначених у пп. 4.2 дисертаційного дослідження. Саме такий підхід дозволить не лише здійснити всебічну оцінку стану підсистеми, але й оцінити вплив загроз невідповідності існуючих параметрів організації безпеки праці законодавчим нормативам на стан системи економічної безпеки будівельних підприємств в цілому.

На стадії підготовки аудитори повинні насамперед зібрати й проаналізувати регламентуючу документацію (положення, інструкції, методики тощо) стосовно об'єкта, який перевірятиметься, на відповідність діючих у підрозділі правил вимогам нормативно-правових актів з охорони праці. Крім того, вони враховують і вивчають всі документи, які стосуються підрозділу, що перевіряється, результати попередніх аудитів, а також нормативно-правові вимоги.

Перевірка використовуваної документації є початковою стадією аудиту, й одержані дані можуть фіксуватися в опитувальному листі. Необхідно переконатися, що вся документація актуалізована, врахована й ідентифікована. В іншому випадку може бути зафіксована невідповідність.

При цьому аудитори можуть проконсультуватися з колективом підприємства й запитати необхідну інформацію. Зокрема, вони повинні одержати точні дані про кадровий склад робітників підрозділу, який перевіряється, а також про його організаційну структуру, підлеглість та розподіл повноважень. За необхідності аудитори уточнюють у керівництва підприємстврм, хто із співробітників братиме участь у перевірці.

В ході вказаного аналізу аудитор визначає теми і блоки питань, враховуючи особливості функціонування підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємств, притаманні саме цьому підрозділу. Головна мета, яку повинен ставити перед собою аудитор, полягає в тому, щоб у результаті проведення перевірки одержати достатній обсяг інформації і даних, який дозволяє чітко встановити:

- чи всі документи та інші дані, які використовуються для опису системи й діяльності підрозділу, е адекватними для досягнення поставлених цілей у сфері охорони праці;

- чи можна стверджувати, що персонал, який перевіряється, має у своєму розпорядженні, розуміє й використовує положення, методики, інструкції та інші діючі документи, які описують правила й вимоги функціонування підсистеми економічної безпеки приорганізації безпеки праці на будівельних підприємствах.

На основі вивчення вказаних документів аудитор складає список базових запитань, які заносить до «Опитувального листа аудиту». Кількість питань не регламентується. До запитань ставиться головна вимога, щоб вони охоплювали в цілому всі теми і види діяльності, які належить перевірити, виходячи з поставленої мети й завдань аудиту. Склад запитань аудиту є комбінацією:

- запитань про наявність організаційно-методичних документів, регламентуючих порядок здійснення робочих процесів;

- запитань для з'ясування, чи ознайомлені працівники із вказаними документами, чи знають вони їх зміст;

- запитань для підтвердження, що виконавці дотримуються поставлених вимог та виконують роботи згідно з методичними вказівками;

- запитань, які дозволяють переконатися, що результати виконуваних виконавцями робіт документуються належним чином.

В процесі проведення аудиту, як правило, виникає необхідність ставити додаткові, що відображають специфіку роботи, конкретизуючі запитання, які аудитор дописує в опитувальний лист у міру виникнення.

Базові опитувальні листи можуть бути заздалегідь передані замовнику для полегшення підготовки до аудиту співробітників підприємства (підрозділу).

Для реалізації поставленого вище завдання, пропонуємо розробити методичний підхід до проведення незалежної оцінки стану підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємств у пп. 5.3 дисертації.

Результати проведення незалежного зовнішнього аудиту підсистеми організації безпеки праці оформлюються у вигляді «висновку аудиту», під яким пропонуємо розуміти документ, який складається аудиторською організацією і містить інформацію про відповідність (невідповідність) об’єкта аудиту вимогам законів та інших нормативно-правових актів з питань безпеки праці [259].

Результати незалежного зовнішнього аудиту підсистеми організації безпеки праці як складова системи економічної безпеки будівельних підприємств пропонуємо подавати у формі висновку, який має містити:

- загальні відомості про об'єкт та замовника аудиту;
- підстави для проведення аудиту, його мету, завдання, програму та обсяг виконаних робіт;
- відомості про аудиторську організацію (аудитора);
- перелік основних законодавчих актів та інших нормативних документів,

на підставі яких та для перевірки на відповідність яким проводився аудит;

- характеристику фактичного стану об'єкта аудиту;

- висновки аудиту щодо виявлених невідповідностей (або відсутності таких) об'єкта аудиту вимогам законодавчих актів та інших нормативних документів;

- відомості щодо підприємств, установ, організацій та осіб, яким надається висновок.

Висновок про проведення аудиту може містити рекомендації щодо заходів, які необхідно вжити для усунення виявлених невідповідностей.

Висновок незалежного зовнішнього аудиту підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємств є офіційним документом, який засвідчується підписом керівника аудиторської організації та печаткою аудиторської організації.

Висновок незалежного зовнішнього аудиту підсистеми організації безпеки праці як складової системи економічної безпеки будівельних підприємств може бути трьох видів:

- негативний висновок видається у разі невідповідності об’єкта аудиту вимогам законів та інших нормативно-правових актів з питань безпеки праці;

- позитивний висновок надається у разі відповідності об’єкта аудиту вимогам законів та інших нормативно-правових актів з питань безпеки праці;

- умовно-позитивний висновок – надається у разі наявності порушень щодо відповідності об’єкта аудиту вимогам законів та інших нормативно-правових актів з питань безпеки праці, які виправлені під час проведення аудиту або протягом місяця.

За результатами проведеного незалежного зовнішнього аудиту видається документ дозвільного характеру, який надається аудиторською організацією суб’єкту господарювання і засвідчує відповідність об’єкта аудиту вимогам законів та інших нормативно-правових актів з питань безпеки праці. Позитивний висновок є підставою для видачі аудиторською організацією свідоцтва щодо відповідності об’єкта аудиту вимогам законів та інших

нормативно-правових актів з питань безпеки праці [54].

Свідоцтво є документом дозвільного характеру з промислової безпеки і охорони праці, який надає право на провадження діяльності суб’єктом господарювання і діє на протязі трьох років.

Після надання свідоцтва аудиторська організація один раз на рік здійснює перевірку діяльності замовника аудиту з питань дотримання ним вимог безпеки праці в тому об'ємі, в якому було надано аудиторський висновок.

У разі отримання суб'єктом господарювання свідоцтва, пропонуємо органам державної влади, до компетенції яких відноситься проведення перевірки діяльності будівельних підприємств в галузі безпеки праці, не здійснюють перевірку таких суб'єктів протягом трьох років після отримання свідоцтва, за виключенням випадків виробничого травматизму зі смертельними наслідками або групових нещасних випадків, викликаних порушенням суб'єктом господарювання умов дотримання безпеки праці.

Список використаних джерел:

1. *Андрієнко В.М. Безпека праці в системі економічної безпеки будівельних підприємств [Текст] : монографія / Андрієнко Василь Миколайович ; Вищ. навч. закл. "Ун-т економіки і права "КРОК". - Київ ; Черкаси : Чабаненко Ю. А., 2014. - 282 с.*
2. *Андрієнко В.М. Організація безпеки праці в системі економічної безпеки будівельних підприємств [Текст] : автореф. дис. ... д-ра екон. наук : 21.04.02 / Андрієнко Василь Миколайович ; ВНЗ "Ун-т економіки та права "КРОК". - Київ, 2015. - 40 с.*

3.2. ПРАКТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КАДРОВОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ

ПОСКРИПКО ЮРІЙ АНАТОЛІЙОВИЧ, *к.е.н.,*
ДАНЧЕНКО ОЛЕНА БОРИСІВНА *д.т.н., доцент,*
завідувач кафедри бізнес-адміністрування та управління проектами,
Університет економіки та права «КРОК»

Персонал будь-якого підприємства може бути джерелом негативних впливів (небезпек, загроз та ризиків) на забезпечення кадрової безпеки підприємств.

Розбіжності поглядів та термінологічні суперечності тлумачення категорій «небезпека», «загроза», «ризик» обумовлюють насамперед необхідність їх уточнення. На думку Є. А. Олейнікова загрозу слід розуміти як «найбільш конкретну і безпосередню форму небезпеки» [5]. Він же зазначає, що небезпека є джерелом загрози, а сама загроза – це «перехід із можливості у реальність» [5]. Автор поділяє точку зору І. П. Мігус та С. М. Лаптєва: «поняття «загроза» являє собою певну подію, що впливає на діяльність суб'єктів господарювання, тоді як «ризик» виступає результатом впливу загроз на господарську діяльність суб'єктів господарювання» [2]. Тобто ризик можна розглядати як імовірність настання загрози. Оскільки загрози виступають як різниця між параметрами середовища і підприємства, таке трактування ризику враховує взаємодію підприємства та зовнішнього середовища та відповідає розумінню сутності економічної безпеки підприємств з позицій системного підходу.

Поділяємо точку зору науковців, які зазначають, що категорії «небезпека», «загроза» та «ризик» пов’язані між собою причинно-наслідковим зв’язком: «небезпека» – це потенційна можливість негативного впливу певних чинників на діяльність підприємства, при якій об’єкт небезпеки не має впливу на її джерело, «загроза» – це існуюча можливість негативного впливу ідентифікованих чинників, дія яких спричинить економічні збитки у разі настання і вимагає відповідної протидії, «ризик» – імовірний результат

наслідків настання загрози, при якій об’єкт ризику може впливати на ризик внаслідок прийняття відповідних рішень. Небезпеки відносяться до минулого або теперішнього часу, загрози – переважно до теперішнього (рідше до минулого), ризики – завжди до майбутнього. На відміну від небезпек, загрози мають суб’єкт та об’єкт, а також спрямованість.

Дослідження сутності суб’єктно-об’єктних відносин кадрової безпеки дозволяє дійти висновку, що в їхній основі містяться загрози, які реалізуються суб’єктом загроз щодо об'єкта безпеки – підприємства. При цьому персонал підприємств може виступати одночасно і як суб’єкт, і як об’єкт загроз.

Негативні впливи (небезпеки, загрози та ризики) на стан забезпечення кадрової безпеки підприємств розподіляють на зовнішні та внутрішні.

До перших відносять: негативний вплив на персонал змін у зовнішньому економічному середовищі, зокрема інфляційних процесів, кращі умови праці і мотивації у конкурентів, налаштованість конкурентів на переманювання топ-менеджерів та провідних співробітників, тиск на співробітників ззовні та їх потрапляння у різні види залежності. До других відносять загрози, пов’язані з низькою ефективністю та реалізацією кадрового потенціалу: неефективна система стимулювання та мотивації, неефективна робота співробітників внаслідок недостатнього освітньо-кваліфікаційного рівня та з інших причин, недостатня організація системи управління персоналом, зокрема навчання персоналу, а прояви деструктивної поведінки персоналу: шахрайство у вигляді привласнення корпоративних коштів («відкати»), крадіжки майна, руйнування морального клімату у колективі, конфліктність, а також специфічні прояви мобінгу, булінгу, харасменту та пресингу за умов відповідної корпоративної культури, недостатнього моніторингу та контролю за співробітниками, а також відсутності системи зворотного зв’яжу при забезпеченні кадрової безпеки.

Кадрові загрози реалізуються через кадрові ризики, наприклад наслідком загроз кращих умов праці і мотивації у конкурентів та установки конкурентів на переманювання співробітників є ризики відтоку кваліфікованих працівників та зростання плинності кадрів.

Попередження загроз і заходи з мінімізації кадрових ризиків необхідно проводити на різних етапах процесу управління персоналом. Наприклад, при загрозі пропозиції кращих умов праці і мотивації у конкурентів та ризику відтоку кваліфікованих працівників необхідно провести комплекс заходів: бенчмаркінг систем мотивації конкурентів та перегляд системи стимулювання та мотивації, визначення недоліків, пріоритетів та заходів з покращення умов праці, оптимізацію соціальних пакетів та забезпечення кадрового резерву.

З метою виявлення та прогнозування негативних впливів на об'єкти забезпечення кадрової безпеки підприємств проводиться моніторинг її показників.

Моніторинг кадрової безпеки дає змогу своєчасно виявити:

– відхилення величин установлених нормативних показників кадрової безпеки у негативний бік;
– збільшення амплітуди динаміки встановлених показників кадрової безпеки на величину, вищу допустимої;
– виникнення небажаних бізнес-процесів, які мають відношення до кадрової безпеки;
– необґрунтовану або деструктивну поведінку окремих співробітників і груп;
– виникнення конфліктних ситуацій між працівниками та із зовнішніми суб'єктами бізнесу (клієнтами, партнерами);
– виявлення надмірної зацікавленості з боку зовнішніх суб'єктів до діяльності підприємства, персоналу, керівництва, інформації тощо;
– виявлення випадків розкрадань, зловживань, пошкоджень майна, зникнення матеріальних цінностей та документів, інших неправомірних дій;
– виявлення спроб несанкціонованого доступу і використання внутрішньої корпоративної інформації.

Одним з ключових завдань підприємств, вирішення яких реалізується за допомогою механізму кадрової безпеки, є своєчасне виявлення загроз та ризиків кадрової безпеки, їх ідентифікація, оцінка впливу та розробка заходів з мінімізації.

Методом експертних оцінок нами визначено наступні основні загрози кадровій безпеці підприємств:

– протиправні дії (або бездіяльність) персоналу по відношенню до підприємства;
– реалізація власних економічних інтересів топ-менеджментом за рахунок підприємства та на шкоду йому;
– корпоративні конфлікти та конфлікти інтересів окремих груп працівників підприємства;
– переманювання топ-менеджерів та ключових працівників підприємств конкурентами;
– напружені відносини в колективі (через психологічну несумісність співробітників, відповідну корпоративну культуру або з інших причин);
– зниження мотивації працівників та продуктивності праці, зростання плинності кадрів;
– зниження задоволеності та лояльності працівників;
– суттєві помилки при наймі на роботу працівників, які не відповідають вимогам до рівня посади;
– зниження кадрового потенціалу до рівня, який недостатній для досягнення стратегічних цілей підприємства;
– зниження конкурентоздатності підприємства за рахунок втрати кадрової переваги.

Проводили оцінку та статистичний аналіз впливу визначених загроз кадровій безпеці у досліджуваній групі підприємств та групі порівняння (n=28 у кожній групі), яку наведено у табл. 3.3.

Таблиця 3.3

Оцінка впливу загроз кадровій безпеці підприємств

№	Показники оцінки								
	X	σ	m	S	V	W	t	p_c	$p_п$
Оцінка по групі підприємств									
Протиправні дії персоналу	4,90	1,25	0,24	1,57	0,25	0,80	-	-	p<0,05
Реалізація власних економічних інтересів	5,26	1,67	0,20	1,36	0,32	0,90	-	-	p<0,05
Корпоративні конфлікти	5,08	0,99	0,19	0,99	0,19	0,90	-	-	p>0,05
Переманювання кращих менеджерів	4,30	1,41	0,27	1,98	0,33	0,80	-	-	p<0,05
Напружені відносини в колективі	4,01	1,12	0,21	1,25	0,28	0,90	-	-	p<0,01
Зниження мотивації та продуктивності	6,29	1,08	0,19	1,17	0,17	0,90	-	-	p>0,05
Зниження задоволен. та лояльності	5,29	1,09	0,21	1,19	0,21	0,90	-	-	p>0,05
Суттєві помилки при наймі на роботу	5,58	0,99	0,18	0,98	0,18	0,90	-	-	p>0,05
Зниження кадрового потенціалу	4,37	0,89	0,22	0,79	0,20	0,90	-	-	p<0,01
Зниження конкурентоздатності	3,08	0,99	0,18	0,99	0,32	0,90	-	-	p>0,05
Оцінка по групі порівняння									
Протиправні дії персоналу	5,64	1,52	0,29	2,31	0,27	0,80	1,98	p<0,05	-
Реалізація власних економічних інтересів	6,14	1,46	0,28	2,13	0,24	0,80	2,50	p<0,05	-
Корпоративні конфлікти	4,89	1,68	0,32	2,84	0,34	0,70	0,51	p>0,05	-
Переманювання кращих менеджерів	5,21	1,31	0,25	1,73	0,25	0,80	2,52	p<0,05	-
Напружені відносини в колективі	5,93	1,09	0,21	1,18	0,18	0,90	6,51	p<0,01	-
Зниження мотивації та продуктивності	6,57	1,48	0,28	2,18	0,23	0,80	0,83	p>0,05	-
Зниження задоволен. та лояльності	5,68	1,19	0,22	1,41	0,21	0,90	1,29	p>0,05	-
Суттєві помилки при наймі на роботу	6,07	1,27	0,24	1,62	0,21	0,80	1,60	p>0,05	-
Зниження кадрового потенціалу	5,39	1,31	0,25	1,72	0,24	0,80	1,71	p<0,01	-
Зниження конкурентоздатності	3,43	1,45	0,27	2,10	0,42	0,80	1,04	p>0,05	-

де: X – середнє арифметичне значення показників, σ – стандартне відхилення, m – похибка стандартного відхилення, S – дисперсія вибірки, V – коефіцієнт варіації, W – коефіцієнт конкордації, t – значення t–критерію Ст'юдента, p_c – вірогідність порівняно із середніми значеннями групи, p_n – вірогідність відносно групи порівняння, p<0,05 статистично вірогідні відмінності; p<0,01 – високий рівень статистичної значущості.

Визначено, що за середніми оцінками по групі підприємств найбільш суттєвими загрозами кадровій безпеці є зниження мотивації та продуктивності праці, зростання плинності кадрів (6,3±0,19) та суттєві помилки при наймі на роботу працівників, які не відповідають рівню посади (5,6±0,18), а також зниження задоволеності й лояльності працівників та реалізація топ-менеджментом власних економічних інтересів за рахунок та на шкоду підприємству. Найнижчий рівень загроз кадровій безпеці становить зниження конкурентоздатності підприємства за рахунок втрати ним кадрової переваги (3,1±0,18). Експерти групи порівняння також відзначають насамперед загрозу зниження мотивації та продуктивності праці (6,6±0,28), а також загрози реалізації топ-менеджментом власних економічних інтересів за рахунок або на шкоду компанії (6,1±0,28) та суттєві помилки при наймі на роботу (6,1±0,24). Середня оцінка по групі підприємств має високий рівень узгодженості думок експертів.

Також проведено оцінку потенційних наслідків впливу загроз кадровій безпеці у досліджуваній групі підприємств та експертну оцінку у групі порівняння (контрольна група), яку наведено у табл. 3.4.

Визначено, що за середніми оцінками по групі підприємств найбільш важливими загрозами, вплив яких виявлятиме найбільш суттєві наслідки, є зниження мотивації та продуктивності праці (9,3±0,11), суттєві помилки при наймі на роботу працівників (9,0±0,11) та зниження задоволеності й лояльності працівників (8,3±0,12). Слід зазначити, що відмінності з групою порівняння не були статистично значущими в жодному випадку, окрім наслідків впливу загрози напружених відносин у колективі, що може свідчити про недостатню увагу до можливих наслідків таких загроз на підприємствах.

Наведені дані демонструють, що для досліджуваних підприємств характерний переважно реактивний підхід щодо протидії загрозам кадровій безпеці, сутність якого полягає у відповідній реакції власників підприємств та топ-менеджменту на фактичні загрози з боку персоналу, що вже виникли.

Таблиця 3.4

Оцінка наслідків впливу загроз кадровій безпеці підприємств

№	Показники оцінки								
	X	σ	m	S	V	W	t	p_c	$p_п$
Оцінка по групі підприємств									
Протиправні дії персоналу	7,98	0,88	0,15	0,77	0,11	0,90	-	-	p>0,05
Реалізація власних економічних інтересів	8,08	0,79	0,12	0,63	0,10	0,90	-	-	p>0,05
Корпоративні конфлікти	6,88	0,76	0,14	0,59	0,11	0,90	-	-	p>0,05
Переманювання кращих менеджерів	7,00	1,08	0,20	1,17	0,15	0,90	-	-	p>0,05
Напружені відносини в колективі	7,42	0,76	0,14	0,57	0,10	0,90	-	-	p<0,05
Зниження мотивації та продуктивності	9,27	0,62	0,11	0,39	0,07	1,00	-	-	p>0,05
Зниження задоволен. та лояльності	8,27	0,65	0,12	0,42	0,08	0,90	-	-	p>0,05
Суттєві помилки при наймі на роботу	8,96	0,55	0,11	0,31	0,06	1,00	-	-	p>0,05
Зниження кадрового потенціалу	8,12	1,02	0,18	1,03	0,13	0,90	-	-	p>0,05
Зниження конкурентоздатності	7,10	1,27	0,21	1,12	0,18	0,90	-	-	p>0,05
Оцінка по групі порівняння									
Протиправні дії персоналу	8,11	1,06	0,20	1,14	0,13	0,90	0,50	p>0,05	-
Реалізація власних економічних інтересів	8,46	1,36	0,25	1,81	0,16	0,80	1,33	p>0,05	-
Корпоративні конфлікти	7,11	1,62	0,31	2,62	0,23	0,70	0,67	p>0,05	-
Переманювання кращих менеджерів	7,36	1,61	0,31	2,61	0,22	0,70	0,97	p>0,05	-
Напружені відносини в колективі	8,07	1,58	0,30	2,51	0,20	0,70	1,97	p<0,05	-
Зниження мотивації та продуктивності	8,89	0,95	0,18	0,91	0,11	0,90	1,77	p>0,05	-
Зниження задоволен. та лояльності	7,96	1,45	0,27	2,11	0,18	0,80	1,03	p>0,05	-
Суттєві помилки при наймі на роботу	8,75	0,96	0,18	0,93	0,11	0,90	1,02	p>0,05	-
Зниження кадрового потенціалу	7,96	1,45	0,27	2,11	0,18	0,80	0,85	p>0,05	-
Зниження конкурентоздатності	6,82	1,41	0,27	2,00	0,21	0,80	0,80	p>0,05	-

де: X – середнє арифметичне значення показників, σ – стандартне відхилення, m – похибка стандартного відхилення, S – дисперсія вибірки, V – коефіцієнт варіації, W – коефіцієнт конкордації, t – значення t–критерію Ст'юдента, p_c – вірогідність порівняно із середніми значеннями групи, p_n – вірогідність відносно групи порівняння, p<0,05 статистично вірогідні відмінності; p<0,01 – високий рівень статистичної значущості.

Слід зазначити, що більш прогресивним є проактивний підхід забезпечення кадрової безпеки, який передбачає планове передбачення загроз та прийняття відповідних рішень щодо реагування (з відповідними заходами та засобами реагування). Своєчасна ідентифікація та попередження загроз значною мірою сприятиме мінімізації негативних наслідків їх настання, таких, як протиправні дії персоналу, реалізація топ-менеджерами власних економічних інтересів за рахунок та шкоду підприємству, зниження кадрового потенціалу.

Оскільки загрози кадровій безпеці реалізуються через відповідні ризики, останні необхідно ідентифікувати та оцінити.

При ідентифікації ризиків кадрової безпеки показник сукупного ризику визначається як сума показників ризиків:

$$R_{êá.} = \sum_{i=1}^{n} H_i \cdot P_i = \sum_{i=1}^{n} R_i , \qquad (1)$$

де: $R_{кб}$ – кількісна оцінка сукупного ризику кадрової безпеки (математичне очікування можливих негативних наслідків настання ризику); R_i – кількісна оцінка і-го ризику; H_i – можливі негативні наслідки у результаті настання і-го ризику; P_i – ймовірність настання і-го ризику (i = 1, 2,…, n).

За своєю сутністю ризики кадрової безпеки передбачають не тільки ідентифікацію та кількісне вираження, але й прийняття рішень щодо реагування та мінімізації (управління ризиками) в умовах невизначеності.

Ключові ризики кадрової безпеки визначали на основних етапах управління персоналом: ризики кадрової безпеки «на вході» в організацію (вхідний контроль), ризики кадрової безпеки «усередині» організації (поточний контроль) та ризики кадрової безпеки «на виході» (вихідний контроль).

Відповідно до наведених етапів проводили ідентифікацію та оцінку ризиків кадрової безпеки на досліджуваних підприємствах і розробку відповідних засобів їх мінімізації (табл. 3.5).

Таблиця 3.5

Ідентифікація ризиків кадрової безпеки та засоби мінімізації

№ п/п	Ризики кадрової безпеки	Засоби мінімізації ризиків
Ризики кадрової безпеки «на вході»		
R1.1	Ризик неправильного вибору джерела пошуку кандидатів (досвід, сфера діяльності, стать, соціальний статус)	Моніторинг ринку праці, сегментація наявних вакансій, скринінг
R1.2	Ризик нечіткого формування вимог до кандидата на вакантну посаду	Взаємодія лінійного менеджера та працівника служби персоналу, чітке формулювання вимог до кандидата
R1.3	Ризик неправильної оцінки кандидата на етапі підбору (недостатня кваліфікація, не виявлення мотивації, несумісність із колективом)	Застосування різноманітних оцінних технологій (як професійної, так і психологічної оцінки) при підборі кандидатів, у т.ч. методики Assessment Center для ключових посад
R1.4	Ризик прийняття кандидата з прямими загрозами економічній безпеці	Ретельна перевірка рекомендацій кандидатів, використання спеціалізованої MIDOT, отримання даних про кандидатів у силових структурах
R1.5	Ризик низької надійності та лояльності кандидата	Ретельна перевірка рекомендацій кандидатів, використання спеціалізованої перевірки MIDOT
Ризики кадрової безпеки «усередині»		
R2.1	Ризик невдалої адаптації працівника у колективі та не сприйняття ним нового працівника	Реалізація програм наставництва для кращої адаптації новачків у колективі
R2.2	Ризик втрати працівником мотивації та стимулів до ефективної праці	Ефективна система матеріального та нематеріального стимулювання, планування ділової кар'єри працівників
R2.3	Ризик відтоку провідних працівників (до конкурентів) через пропозицію кращих умов роботи	Ефективна система матеріального та немат. стимулювання, планування ділової кар'єри працівників, програми розвитку
R2.4	Ризик зловживань працівника (службові порушення, фінансові зловживання, розповсюдження комерційної інформації)	Моніторинг, контроль діяльності та попередження можливих неправомірних дій персоналу менеджерами, службами управління персоналом та безпеки
R2.5	Ризик припинення розвитку та втрата кадрового потенціалу працівниками підприємств	Впровадження стратегії постійного розвитку та навчання персоналу на основі оцінки та атестації працівників
R2.6	Ризик виникнення внутрішніх конфліктів між працівниками підприємств	Чітка система внутрішніх комунікацій, розподіл повноважень, розвиток корпоративної культури та ідентичності
R2.7	Ризик зниження задоволеності, лояльності та благонадійності працівників підприємств	Визначення та корекція причин зниження задоволеності, лояльності та благонадійності, ротація, використання спеціалізованої перевірки MIDOT

№ п/п	Ризики кадрової безпеки	Засоби мінімізації ризиків
Ризики кадрової безпеки «на виході»		
R3.1	Ризик фінансових претензій працівника до підприємства (у разі неправомірного звільнення)	Дотримання вимог чинного трудового законодавства
R3.2	Ризик формування негативного іміджу підприємства як роботодавця через розповсюдження працівниками негативної інформації про нього	Консультування співробітника, що звільняється, щодо стану ринку праці, допомога в складанні резюме, позитивні рекомендації
R3.3	Ризик поширення працівником важливої комерційної інформації про підприємство серед його конкурентів	Підписання угоди про нерозповсюдження комерційної таємниці при прийнятті на роботу, інформаційна та юридична робота з працівником служби економічної безпеки, вихідне тестування

Для кожного з ідентифікованих ризиків необхідно розробити комплекс заходів з його мінімізації (та попередження) та визначено відповідальних.

Ідентифіковані ризики кадрової безпеки «на вході» в організацію (контроль на вході), ризики «усередині» організації (контроль у процесі) та ризики «на виході» вимагають відповідної оцінки (табл. 3.6).

Таблиця 3.6

Оцінка ризиків на різних етапах забезпечення кадрової безпеки підприємств

№	Ризики	Підприємства									Середнє значення		
		ТОВ 1			ТОВ 2			ТОВ 3					
		О	В	Р	О	В	Р	О	В	Р	О	В	Р
Ризики кадрової безпеки «на вході» в організацію													
1	R1.1	0,22	0,3	0,07	0,21	0,1	0,02	0,24	0,2	0,05	0,22	0,2	0,04
2	R1.2	0,27	0,4	0,11	0,29	0,5	0,15	0,14	0,3	0,04	0,23	0,4	0,09
3	R1.3	0,55	0,7	0,39	0,48	0,8	0,38	0,49	0,8	0,39	0,51	0,8	0,39
4	R1.4	0,64	0,9	0,58	0,59	0,9	0,53	0,47	0,9	0,42	0,57	0,9	0,51
5	R1.5	0,61	0,8	0,49	0,57	0,8	0,46	0,52	0,7	0,36	0,57	0,8	0,43
6	Rc1	0,46	0,6	0,28	0,43	0,6	0,27	0,37	0,6	0,22	0,42	0,6	0,25
Ризики кадрової безпеки «усередині» організації													
7	R2.1	0,59	0,6	0,35	0,56	0,5	0,28	0,54	0,3	0,16	0,56	0,5	0,26
8	R2.2	0,68	0,7	0,48	0,69	0,9	0,62	0,65	0,5	0,33	0,67	0,7	0,47
9	R2.3	0,71	0,7	0,50	0,67	0,9	0,60	0,73	0,7	0,51	0,70	0,8	0,54
10	R2.4	0,49	0,6	0,29	0,51	0,5	0,26	0,45	0,5	0,23	0,48	0,5	0,26
11	R2.5	0,76	0,6	0,46	0,70	0,7	0,49	0,55	0,5	0,28	0,67	0,6	0,40
12	R2.6	0,65	0,7	0,46	0,49	0,5	0,25	0,45	0,3	0,14	0,53	0,5	0,27
13	R2.7	0,68	0,6	0,41	0,60	0,7	0,42	0,49	0,5	0,25	0,59	0,6	0,35
14	Rc2	0,65	0,6	0,42	0,60	0,7	0,40	0,55	0,5	0,26	0,60	0,6	0,36

№	Ризики	Підприємства									Середнє значення		
		ТОВ 1			ТОВ 2			ТОВ 3					
		О	В	Р	О	В	Р	О	В	Р	О	В	Р
Ризики кадрової безпеки «на виході» із організації													
15	R3.1	0,13	0,3	0,04	0,19	0,3	0,06	0,21	0,4	0,08	0,18	0,3	0,06
16	R3.2	0,35	0,3	0,11	0,27	0,4	0,11	0,39	0,5	0,20	0,34	0,4	0,13
17	R3.3	0,39	0,5	0,20	0,34	0,3	0,10	0,35	0,7	0,25	0,36	0,5	0,18
18	Rc3	0,29	0,4	0,12	0,27	0,3	0,08	0,32	0,5	0,16	0,29	0,4	0,12
Середні значення													
19	Rc1-3	0,47	0,6	0,26	0,43	0,5	0,23	0,41	0,5	0,21	0,44	0,5	0,23

де: О – оцінка ймовірності настання ризиків; В – оцінка впливу негативних наслідків у разі настання ризиків; Р – оцінка ризиків; R - ризики відповідно до табл. 3 та їх середні значення (Rc).

Аналіз ризиків кадрової безпеки пропонуємо проводити за запропонованими критеріями їхньої оцінки (табл. 3.7).

Таблиця 3.7

Критерії оцінки ризиків кадрової безпеки підприємств

№	Рівень	дуже низький	низький	середній	високий	дуже високий
1	Оцінка ймовірності настання ризику	0-0,19	0,2-0,39	0,4-0,69	0,7-0,89	0,9-1
2	Оцінка впливу негативних наслідків у разі настання ризику	0-0,19	0,2-0,39	0,4-0,69	0,7-0,89	0,9-1
3	Зважена оцінка	<0,2	0,2-0,39	0,4-0,69	0,7-0,8	>0,81

Основними ризиками КБ «на вході» в організацію виступають ризик прийняття кандидата з прямими загрозами економічній безпеці (R1.4, 0,51, середній ризик), ризик низької надійності та лояльності кандидата (R1.5, 0,43, середній ризик) та ризик неправильної оцінки кандидата на етапі підбору (R1.3, недостатня кваліфікація, не виявлення реальної мотивації кандидата, психологічна несумісність із колективом; 0,39, низький ризик).

Основними засобами мінімізації ризиків кадрової безпеки підприємств є здійснення ретельної перевірки рекомендацій кандидатів, використання

спеціалізованих тестів MIDOT «на вході», отримання даних про кандидатів у силових структурах. Також засобами мінімізації даних ризиків є застосування різноманітних оцінних технологій (як професійної, так і психологічної оцінки) при підборі кандидатів.

Найбільшими ризиками кадрової безпеки «усередині» організації є ризик відтоку провідних працівників через пропозицію кращих умов роботи (R2.3, 0,54, середній ризик), ризик втрати працівником мотивації та стимулів до ефективної праці (R2.2, 0,47, середній ризик) та ризик припинення розвитку і втрата кадрового потенціалу працівниками (R2.5, 0,40, середній ризик).

Основними методами та засобами мінімізації даних ризиків є впровадження ефективної системи матеріального та нематеріального стимулювання, розробка та впровадження стратегії і програм планування ділової кар'єри працівників, розвитку персоналу з необхідним виділенням матеріальних ресурсів.

Основними ризиками кадрової безпеки «на виході» з організації є ризик витоку та поширення працівником, що звільняється, важливої комерційної інформації про підприємство серед його конкурентів (R3.3, 0,18) та ризик формування негативного іміджу підприємства як роботодавця через розповсюдження працівниками негативної інформації про нього (R3.2, 0,13), проте рівень таких ризиків дуже низький, а їх настання малоймовірне.

Засобами мінімізації даних ризиків є інформаційно-консультаційна підтримка працівників, які звільняються: консультування про стан ринку праці, допомога в складанні резюме, надання об'єктивних рекомендацій тощо.

Загалом рівень ризиків кадрової безпеки досліджуваних підприємств «на вході» є низьким (0,25, низький ризик), порівняно вищі показники ризиків кадрової безпеки «усередині» організації (0,36 бали, низький ризик), а ризики кадрової безпеки «на виході» є дуже низькими та їх настання малоймовірне (0,12 балів).

Визначення ризиків та загроз кадровій безпеці шляхом проведення оцінок кандидатів та періодичних оцінок співробітників передбачає Євростандарт

ISO/IEC 27002 [7]. Зокрема у розділі 8 «Безпека кадрових ресурсів», ст. 8.1 «Перед наймом», зазначається, що оцінка кандидата / співробітника повинна гарантувати, що кандидати / співробітники розуміють свою відповідальність і відповідають своїм посадам, а також бути спрямованою на зниження ризику крадіжок, шахрайства або неправомірного використання устаткування: «усі кандидати на роботу підлягають відповідній перевірці, особливо для відповідальних посад» [7].

Згідно зі ст. 8.1.2 «Перевірка кандидатів», якщо робота, незалежно від того, чи є це первинним призначенням або підтвердженням по службі, припускає доступ співробітника до коштів, обробки інформації, і зокрема, якщо інформація становить комерційну таємницю, наприклад, фінансова або конфіденційна інформація, то організація повинна розглянути можливість проведення подальших і більш детальних перевірок кандидатів.

Вимоги до фахових компетенцій співробітників є необхідною, але не достатньою умовою стабільного розвитку підприємств, оскільки персонал може не тільки забезпечувати конкурентоздатність підприємства, але й бути його руйнівником. Тобто тільки фахові вимоги до персоналу не враховують ризики та загрози, джерелом яких може бути деструктивна поведінка персоналу, а отже тільки фахове тестування не спроможне забезпечити кадрову безпеку на підприємствах. Тому підвищення ефективності забезпечення кадрової безпеки повинно ґрунтуватися на інтегрованому управлінні економічною безпекою та персоналом. Це особливо актуально для малих та середніх підприємств, які є менш захищеними та більш вразливими до негативного впливу як зовнішніх, так і внутрішніх ризиків.

Кадрова безпека є функціональною підсистемою одразу двох систем підприємства: системи економічної безпеки та системи управління персоналом, тому вона повинна бути інтегрована з ними, що сприятиме підвищенню ефективності управління персоналом у розрізі мінімізації ризиків і запобігання загрозам та максимізації соціально-економічної ефективності діяльності підприємств. З цією метою проводиться оцінка кандидатів та співробітників

компаній. За нашими даними [4], на малих та середніх підприємствах традиційні інтерв'ю та співбесіди застосовуються у 100% випадків, анкетування в середньому – у 70%, скринінг – у 60%, перевірка рекомендацій – у 50%, моделювання ситуацій ділової практики – у 75%, перевірка теоретичних знань кандидатів – у 40%, тестування з визначення рівня IQ / EQ – у 3,3%, особистісні тести – в 6,7%, Assessment Center – у 3,3%, нестандартні та додаткові методи оцінки – в 6,7%. Слід зауважити, що сучасні спеціалізовані діагностичні методики забезпечення кадрової безпеки на досліджуваних підприємствах не застосовувались.

Практичний досвід демонструє, що на малих та середніх підприємствах спостерігається тенденція до застосування переважно «простих» оціночних методик. Обмежене застосування більш ефективних, з точки зору забезпечення кадрової безпеки оціночних процедур, не сприяє відбору кандидатів, професійні та особистісні якості яких в достатній мірі повній мірі відповідають вимогам кадрової безпеки, у кінцевому рахунку може створити загрозу досягненню стратегічних цілей організації.

Влучну характеристику цій обставині дав відомий менеджер та бізнесмен Уорен Баффет (Warren Buffett): «Коли ви наймаєте працівника, ви розраховуєте на його чесність (відвертість), професійні знання (інтелект) та ділову активність. Але, якщо не буде першого, дві останні знищать ваш бізнес» [6].

З огляду на вищенаведене, ефективними з точки зору забезпечення кадрової безпеки можна розглядати саме спеціалізовані методики, такі як перевірка на детекторі неправди (поліграфі) та тести компанії MIDOT.

Основними сферами використання детекторів неправди (поліграфів) є корпоративні розслідування, отримання додаткової інформації в процесі розслідування, забезпечення об'єктивності та оцінка достовірності повідомленої кандидатом інформації. Поліграф використовується переважно для виявлення та розкриття корпоративних правопорушень [3].

Періодичні перевірки з використанням поліграфа допомагають виявити скоєні правопорушення, зв'язки з кримінальним світом, конкурентами тощо.

При розкритті скоєних правопорушень застосування поліграфа дозволяє звузити коло підозрюваних, встановити осіб, причетних до правопорушення та з'ясувати його обставини, а також усунути підозру в причетності до нього та виявити лжесвідчення [3].

В той же час, детекція неправди є логічним тестом і не стосується внутрішньої мотиваційної сфери працівника [1]. Основними чинниками, які обмежують застосування поліграфів на підприємствах є негативне психологічне відношення співробітників, які сприймають поліграфи переважно як «детектори брехні», а сам процес детекції як прояв недовіри, тому їх часте та тривале застосування може спричинити негативні соціальні наслідки у колективі. Застосування поліграфів вимагає високої фаховості, навичок роботи та значного досвіду. Певним чином обмежує застосування поліграфів наявність методів його обману, суб'єктивність та можливість зовнішнього впливу на поліграфологів, а також тривалість і висока вартість процедури детекції [1].

Та основним недоліком, який обмежує широке застосування методу детекції неправди з метою забезпечення кадрової безпеки, є його низька прогностична цінність – поліграф з високою імовірністю може підтвердити події минулого («було – не було»), але не має сенсу при застосуванні з метою прогнозування потенційних ризиків («буде – не буде») [1].

Однією з сучасних діагностичних та прогностичних методик, яка застосовується з метою прогнозування потенційних ризиків та суттєво розширює можливості забезпечення кадрової безпеки, є система MIDOT, яка розроблена вченими та практиками полі графологами і психологами. Система MIDOT є серією психологічних тестів, які оцінюють морально-етичні судження людини, на підставі аналізу яких виконується виявлення та прогнозування потенційних ризиків деструктивної поведінки співробітників у майбутньому [1, 8].

Оцінка благонадійності кандидата та оцінка ризиків деструктивної поведінки кандидата на роботу виконуються за допомогою тестів IntegriTEST та StabiliTEST, оцінка благонадійності співробітника та періодична оцінка

ризиків деструктивної поведінки серед співробітників виконуються за допомогою тесту TRUSTEE, організаційні дослідження та оцінка ризиків і виявлення ознак деструктивної поведінки на рівні організаційних підрозділів виконуються за допомогою тестів ProEthic View та IntegriEXIT [8].

Тести MIDOT компанії MidotSystem дозволяють дистанційно та швидко (проходження тесту до 30 хвилин) отримати результат, який з великим ступенем достовірності дозволить оцінити кандидатів за шкалами (параметрами): «відвертість» (оцінка готовності повідомляти правдиву інформацію або схильності спотворювати інформацію), «крадіжка» (оцінка ступеню схильності або стійкості до розкрадання власності компанії), «хабар» (оцінка ступеню схильності або стійкості до хабара або підкупу), «корпоративні норми» (оцінка готовності дотримуватися корпоративних соціальних норм та стандартів або схильність їх порушувати), «особистісні якості» (оцінка готовності до сумлінного виконання службових обов'язків або схильності бути нетерплячим, агресивним), «залежності» (оцінка ступеню схильності до вживання та роботи під впливом алкоголю і наркотиків) [1, 8].

Важливою особливістю тестів MIDOT є те, що вони не призначені для оцінки професійних та ділових якостей (це вирішується за допомогою загальних та спеціалізованих методик), а є методикою оцінки суджень морально-етичного характеру людини. На відміну від тестування на поліграфі, яке з високою вірогідністю підтверджує певні факти минулого та відношення до них особи, яка тестується, MIDOT дозволяє з високою вірогідністю прогнозувати типологію поведінки і відповідно розраховувати (чи не розраховувати) на надійність та порядність співробітників в майбутньому в плані їх відповідності корпоративним морально-етичним нормам [1].

Оцінка MIDOT є етичною процедурою та не суперечить діючому законодавству України (згідно до ст. 21, 26, 40, 41, 130, 139 ТК України, ст. 36 ГК України).

Результати тестів, зокрема тесту для оцінки благонадійності кандидатів на роботу IntegriTEST, характеризуються високою надійністю та стабільністю.

Коефіцієнт відтворюваності результатів (загальної оцінки) при повторному тестуванні через 2–8 тижнів становить 0,70 від загальної оцінки, отриманої після першого тестування, і 0,75 від оцінок по параметрах, отриманих після першого тестування.

Проведені дослідження валідності тестів IntegriTEST продемонстрували його високу змістовну валідність відносно результатів поліграфа: в групі 1 протестовані за допомогою IntegriTEST та поліграфу 596 кандидатів (кореляція становить до 0,89), в групі 2 протестовані за допомогою IntegriTEST та перевірені службою безпеки 247 кандидатів (відповідність у 85% випадків, кореляція 0,52), в групі 3 порівняні результати двох перевірок на поліграфі (проміжок 6–18 місяців). Частина вибірки (57 осіб) складалася з кандидатів, прийнятих на роботу з результатами перевірки IntegriTEST, а частина (90 осіб) – без такої перевірки. Працівники, найняті після перевірки IntegriTEST, у 5 разів менше «провалювали» повторну перевірку на поліграфі у порівнянні з групою працівників, які не проходили перевірку IntegriTEST (табл. 3.8).

Проведено оцінку організаційної надійності, а також оцінку ризику службових зловживань співробітників досліджуваних підприємств за допомогою тестів IntegriTEST та TRUSTEE за методикою MIDOT з метою визначення ризику службових зловживань та оцінки благонадійності і лояльності діючих працівників за критеріями (група показників «Особистісні цінності»):

– шкала «Відвертість», діапазон: від схильності брехати або спотворювати інформацію до схильності повідомляти правдиву інформацію;

– шкала «Розкрадання», діапазон: від схильності до крадіжки корпоративних грошей, майна, отримання «відкатів» до бережливого ставлення до фінансових ресурсів та майна організації;

– шкала «Організаційна толерантність», діапазон: від проявів агресивності, нечемності, конфліктогенності до проявів ввічливості, терплячості, безконфліктності;

– шкала «Корпоративні норми», діапазон: від схильності до порушення корпоративних норм, стандартів, правил та інструкцій до дотримання корпоративних норм, стандартів, правил та інструкцій.

Таблиця 3.8

Оцінка валідності тесту IntegriTEST за методикою MIDOT

№	Integritest / MIDOT	Рекоменд. + середній	Не рекоменд.	Всього
Група 1				
1	Рекомендований після перевірки на поліграфі	522	8	530
2		87,6%	1,3%	88,9%
3	Не рекомендований після перевірки на поліграфі	5	61	66
4		0,8%	10,2%	11,1%
5	Всього	527	69	596
6		88,4%	11,6%	100%
Група 2				
7	Рекомендований після перевірки на поліграфі	215	19	234
8		87,1%	7,7%	94,7%
9	Не рекомендований після перевірки на поліграфі	2	11	13
10		0,8%	4,5%	5,3%
11	Всього	217	30	247
12		87,9%	12,1%	100%
Група 3				
13	Рекомендований після перевірки на поліграфі	55	73*	128
14		37,4%	49,7%	87,1%
15	Не рекомендований після перевірки на поліграфі	2	17*	19
16		1,4%	11,6%	12,9%
17	Всього	57	90*	147
18		38,8%	61,2%	100%

** в групі 3 – не тестувалися [1].*

Принцип оцінки ризику службових зловживань за методикою MIDOT досить простий і не потребує спеціальної фахової підготовки, результати тестів нескладні для інтерпретації та не вимагають додаткових навичок або залучення фахівців – чим вища оцінка, тим нижчий ризик. Оцінка ризику службових зловживань вираховується за допомогою комп’ютерного алгоритму автоматично. Значення знаходяться у шакалах від 0 до 100 балів. За результатами тестування ризик може бути оцінений як: малоймовірний,

низький, середній або високий (за кожним окремим кандидатом або співробітником).

Для можливості порівняння результатів між співробітниками, групами, підприємствами та між собою в динаміці, запропоновано використовувати коефіцієнт порівняння, який пропонується розраховувати як середнє значення показників основних шкал «Розкрадання», «Толерантність у роботі» та «Корпоративні норми» (переведені для зручності у децимальну або сантимальну шкалу) помножених на показник шкали «Відвертість» (наведений в діапазоні 0–1) [1]. Такий коефіцієнт за результатами тестування може набувати значень від 1 до 8,1 (чим його значення вище, тим краще позитивна ознака та нижчий ризик). Довірча імовірність приймалась рівною 0,95 при статистично вірогідних (значимих) відмінностях $p<0,05$.

Результати оцінки ризику службових зловживань аналізованої групи підприємств за методикою MIDOT наведено у табл. 3.9.

Таблиця 3.9

Оцінка ризику службових зловживань за методикою IntegriTEST / MIDOT на підприємствах

	Підприємства / Показники	ТОВ 1	ТОВ 2	ТОВ 3	Середнє значення
1	Відвертість	6,6 ± 0,14	7,4 ± 0,22	7,3 ± 0,20	7,1 ± 0,13
2	Розкрадання	6,9 ± 0,35	7,1 ± 0,27	7,4 ± 0,31	7,1 ± 0,22
3	Організаційна толерантність	6,8 ± 0,29	6,8 ± 0,27	6,7 ± 0,26	6,8 ± 0,17
4	Корпоративні норми	7,4 ± 0,32	6,5 ± 0,36	7,2 ± 0,37	7,0 ± 0,24
5	Середня оцінка	6,92	6,95	7,16	7,01
6	Коефіцієнт порівняння	4,65	5,02	5,21	4,96

Наведено середньоарифметичні оцінки у балах та середньоквадратичні (стандартні) відхилення оцінок.

За результатами оцінки ризику службових зловживань співробітників досліджуваних підприємств за методикою MIDOT визначено, що статистично вірогідні відмінності ($p<0,05$) або високий рівень статистичної значимості ($p<0,01$) відносно середніх значень не відмічалися. В даному випадку це має позитивне значення, оскільки така ситуація в цілому свідчить про однорідність

кадрового складу досліджуваних підприємств з точки зору надійності та порядності співробітників та їх відповідності корпоративним морально-етичним нормам з точки зору забезпечення кадрової безпеки.

Децимальна інтервальна шкала оцінок може набувати значень від 0 до 10, де оцінки: 0–2 – дуже низькі; 2–4 – низькі; 4–6 – середні; 6–8 – високі; 8–10 – дуже високі. Чим вище бал – тим краще позитивна ознака та нижчий ризик.

Співробітники досліджуваних підприємств в цілому відверто відповідали на запитання (7,1 ± 0,13 бали за шкалою «Відвертість»).

Результати тестування за шкалою «Розкрадання» виявили низьку імовірність можливої крадіжки корпоративних грошей, майна, цінностей та отримання «відкатів» та демонстрували переважно бережливе ставлення до фінансових ресурсів і майна організації (7,1 ± 0,22 бали). На цей показник слід звернути особливу увагу, оскільки саме отримання неправомірної фінансової винагороди у вигляді «відкатів» є одним з поширених та важко ідентифікуємих корпоративних порушень з боку топ-менеджменту вітчизняних підприємств.

Результати тестування за шкалою «Організаційна толерантність» виявили порівняно низький рівень агресивності і конфліктогенності та прагнення до ввічливості і безконфліктності персоналу досліджуваних підприємств. Це свідчить, що у звичайних умовах, співробітники проявляють готовність до ввічливості та уникненню конфліктів у роботі (6,8 ± 0,17 бали).

За шкалою «Корпоративні норми» визначено, що співробітники досліджуваних підприємств в цілому демонстрували схильність до дотримання корпоративних норм, стандартів, правил та інструкцій (7,0 ± 0,24 бали).

Результати оцінки ризику службових зловживань за методикою MIDOT свідчать, що в цілому, ризик службових зловживань співробітників досліджуваних підприємств можна оцінити як малоймовірний. Середня оцінка в групі становить 7,01 балів, по підприємствах: А – 6,92 балів, В – 6,95 балів та С – 7,16 балів, що відповідає діапазону високих оцінок в цілому та є непоганим показником для підприємств (для деяких фінансових установ мінімально допустимий рівень оцінюється у 5,0–5,5 балів за децимальною шкалою).

Використання версії TRUSTEE / MIDOT надає додаткові можливості оцінки співробітників за групою показників «Організаційні умови»:

– шкала «Організаційна прихильність», діапазон: від неприхильності та незалученості до організаційної прихильності та залученості;

– шкала «Безпека компанії», діапазон: від усвідомлення та виконання вимог безпеки до не усвідомлення та невиконання вимог безпеки.

За результатами оцінки «Організаційних умов» за методикою TRUSTEE / MIDOT встановлено, що середня оцінка показнику «Організаційна прихильність» становила 7,8 балів, а середня оцінка показнику «Безпека компанії» – 6,8 балів (в середньому значення показників «Організаційні умови» – 7,3 бали), що є достатньо високими значеннями.

При детальному аналізі результатів виявлено, що «внутрішня» структура ризиків співробітників відрізняється: одні з них пов'язані зі схильністю до зловживань своїм службовим становищем, інші – комбінацією такої схильності та наявності обставин. Також встановлено, що в поодиноких випадках співробітники ухилялись від конкретних відповідей на запитання та один із співробітників був схильний до порушення корпоративних норм та спотворення інформації (результат графічної частини тесту TRUSTEE / MIDOT цього співробітника наведено на рис. 3.3).

Результати оцінки співробітника за методикою TRUSTEE / MIDOT свідчать, що він може виявляти ввічливість та терплячість по відношенню до колег, охайно ставитися до корпоративного майна та виявляти стійкість до розкрадання власності компанії (по 7,5 бали), проте за певних умов може бути схильним до порушення корпоративних норм, правил та посадових інструкцій та схильним до спотворення інформації (по 5,5 бали). Він може виявляти організаційну прихильність та замученість, бути командним гравцем (по 7,1 бали), але не усвідомлює повною мірою та може не виконувати вимоги щодо економічної безпеки підприємства. Текстова частина містить деталізовані коментарі по наведених даних. Загальна оцінка – співробітник має середній

ризик здійснення службового зловживання або порушення корпоративних норм, правил та інструкцій.

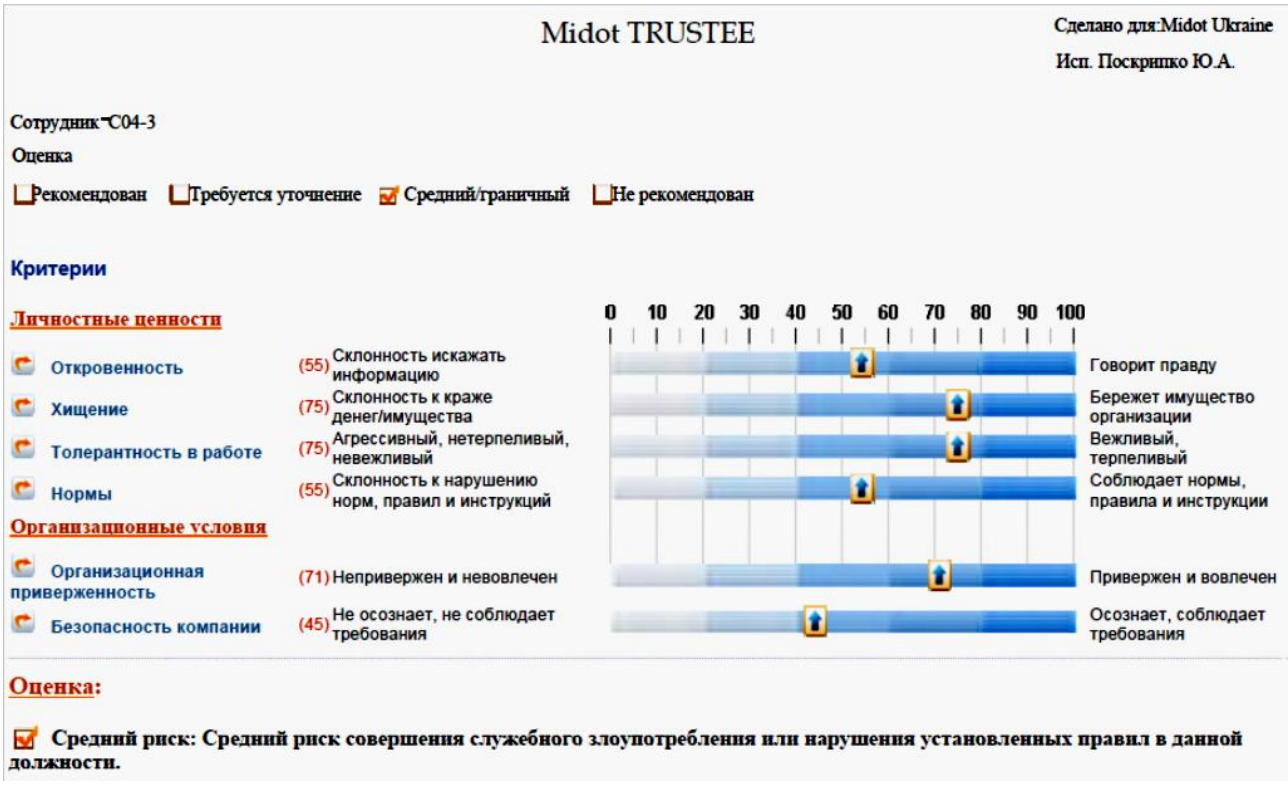


Рис 3.3. Графічна частина звіту результату тесту TRUSTEE / MIDOT

Для співробітників, які за результатами оцінки потрапляють до «зони середнього ризику», рекомендовано призначення супервайзера для моніторингу діяльності співробітників (зокрема фінмоніторингу), повторне тестування через визначений період. Для співробітників, які знаходяться в «критичній зоні» – призначення персонального аудиту, підготовка кадрового резерву та прийняття рішення про подальшу співпрацю за результатами аудиту.

За допомогою комп’ютерної програми [9] нами розраховано показники економічної доцільності застосування методики MIDOT, які наведено у табл. 3.9.

Таблиця 3.9

Економічне обґрунтування застосування методики MIDOT на підприємствах

№	Підприємства / Показники	ТОВ 1	ТОВ 2	ТОВ 3	Середнє значення
1	Потенційні збитки (всього за рік, $)	8 760	5 310	23 760	12 610
2	Потенційні заощадження (всього, $)	1 752	1 062	4 752	2 522
3	Витрати на Assessment (всього, $)	640	360	1 690	897
4	Рентабельність інвестицій, ROI ($)	1 112	702	3 062	1 625
5	Рентабельність інвестицій, ROI (%)	174	195	181	183

За результатами оцінки наведеними у табл. 3.9 встановлено, що застосування методики MIDOT в процесі забезпечення кадрової безпеки на підприємствах є доцільним та економічно обґрунтованим. Воно дозволяє уникнути потенційних збитків на підприємствах в середньому у сумі $ 12 610 за рік та заощадити $ 2 522 за аналогічний період, при цьому рентабельність інвестицій ROI становить в середньому 183%.

Таким чином, діяльність вітчизняних підприємств супроводжується постійним впливом несприятливих чинників, зокрема кадрових загроз та ризиків, які повинні бути ідентифіковані. Розглянуто можливості оцінки загроз та ризиків з боку персоналу в процесі забезпечення кадрової безпеки, зокрема можливості застосування сучасних діагностичних та прогностичних систем, таких як система MIDOT у забезпеченні кадрової безпеки на підприємствах. Наведено результати оцінки ризику службових зловживань співробітників досліджуваних підприємств за методикою IntegriTEST і TRUSTEE / MIDOT. Встановлено, що ризик службових зловживань співробітників досліджуваних підприємств можна оцінити як малоймовірний, а показники оцінки за групами характеристик – достатньо високими. Тестування MIDOT в процесі забезпечення кадрової безпеки допомагає зменшити ризик значних витрат на різних етапах процесу управління персоналом та заощадити бюджетні кошти за рахунок попередження шкоди та збитків з боку персоналу.

Список використаних джерел:

1. Городницький Б. Б. Сучасні діагностичні можливості забезпечення кадрової безпеки / Б. Б. Городницький, Ю. А. Поскрипко // Економіка і фінанси. – № 5. – 2015. – С. 33 – 44.

2. Мігус І. П. Необхідність розмежування понять «загроза» та «ризик» при діагностиці економічної безпеки суб'єктів господарювання / І. П. Мігус, С. М. Лаптєв // Ефективна економіка. – 2011. – № 12. – [Електронний ресурс]. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=821.

3. Мігус І. П. Сучасні підходи до оцінки персоналу суб'єктів господарювання з позицій економічної безпеки / І. П. Мігус, С. А. Черненко // Бізнес-інформ, 2013. – № 10. – С. 357 – 363.

4. Поскрипко Ю. А. Оценка персонала в практике кадровой безопасности малых и средних предприятий / Ю. А. Поскрипко // Социально-гуманитарный вестник Юга России. – №8. – 2013. – С. 142 – 153.

5. Экономическая и национальная безопасность: Учебник / Под ред. Е. А. Олейникова. – М.: Издательство «Экзамен», 2005. – 768 с.

6. Buffett W. [Електронний ресурс]. – Режим доступу: http://www.businessinsider.com/warren-buffett-hiring-strategy-2014-10.

7. ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls (second edition) [Електронний ресурс]. – Режим доступу: http://www.iso27001security.com/html/27002.html.

8. Midot: офіційний сайт [Електронний ресурс]. – Режим доступу: http://www.midot.com.

9. Midot: ROI Calculator [Електронний ресурс]. – Режим доступу: http://www.midot.com/roi-calculator.

3.3. КОНЦЕПТУАЛЬНИЙ ПІДХІД ДО ОЦІНКИ РІВНЯ ДІЛОВОЇ РЕПУТАЦІЇ БАНКУ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ БАНКУ

АНДРУСЯК НАТАЛІЯ ОЛЕКСАНДРІВНА, *к.е.н., доцент,*
доцент кафедри економіки підприємства, обліку і ауиту
Черкаського національного університету ім. Богдана Хмельницького
ГОНЧАРОВА КРІСТІНА ГЕОРГІЇВНА*, здобувач*
кафедри менеджменту та економічної безпеки
Черкаського національного університету ім. Богдана Хмельницького

Концепція оцінки рівня ділової репутації полягає у об’ємній оцінці, як нематеріальної складової топ-менеджменту банку так і матеріальну складову банку «гудвіл». Тобто, оцінювати потрібно, як фізичну особу – топ – менеджера банку так і юридичну– банківську установу.

Репутація банківської установи – поняття багатогранне і складне, всі її компоненти пов'язані між собою і тільки в комплексі можуть забезпечити повноцінну методологічну оцінку.

Ділова репутація має значення головним чином для суспільства, адже саме воно є головним і неупередженим суб’єктом її оцінки. Система комплаєнс в свою чергу, є частиною корпоративної культури Банківської установи та входить до системи внутрішньобанківського контролю, а отже є елементом системи економічної безпеки банку.

Наукова позиція стосовно гудвіл є наступною: матеріальна стаття може формуватися за оцінкою ефективності роботи системи комплаєнс банківської установи, що регламентується законодавством України та нормативно - правовими актами Базельського Комітету з питань банківського нагляду.

Концептуальний підхід до оцінки ділової репутації топ- менеджменту банку (рисунок 3.4) має проводитись за наступних підходів:

- оцінка претендента на посаду топ –менеджера банку,
- оцінка діючого топ- менеджменту банку.

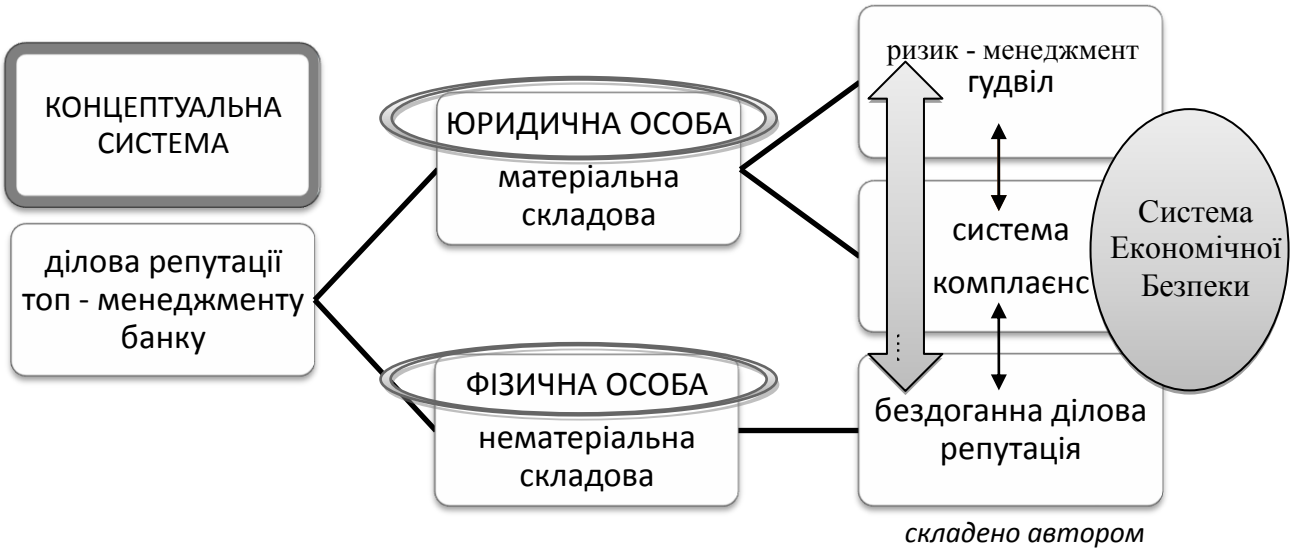


Рис. 3.4. Структура концептуальної оцінки рівня ділової репутації топ – менеджменту банку

Оцінка претендента на посаду топ –менеджера банку має проводитись за критеріями НБУ.

Розглянемо репутаційну безпеку в системі економічної безпеки банку, а саме елементи, що їй відповідають згідно нашої моделі внутрішньобанківського контролю, отже репутаційна безпека забезпечується наступними елементами системи внутрішньобанківського контролю, а саме: система комплаєнс, система фінансового моніторингу, система інформаційної –безпеки.

Моніторинг та контроль рівня системи фінансового моніторингу та системи забезпечується комплаєнс ризик менеджментом.

Моніторинг та контроль рівня системи інформаційної –безпеки забезпечується операційно - технологічним ризик менеджментом, яка дуже часто за структурою входить до підрозділу комплаєнс.

Концептуальний підхід до оцінки ділової репутації діючого топ-менеджменту банку в системі економічної безпеки банку, а саме системі внутрішньобанківського контролю має складатися з наступних елементів:

- Оцінка рівня ділової репутації топ – менеджменту банку за критеріями НБУ,

- Оцінка рівня ділової репутації банку за наступними критеріями:
  -гудвіл,
-ефективність системи комплаєнс,
  -рейтингові оцінки ЗМІ.

Концепція системної оцінки ділової репутації розглядає

- гудвіл, як кількісний показник,
- ефективність системи комплаєнс, як якісний показник,

Системна оцінка гудвіл припускає можливість

- оцінки гудвілу при продажу банку,
- бухгалтерська стаття «гудвіл», що формується та ведеться внутрішньобанківським обліком.

Оцінка ефективності системи комплаєнс банку є маловивченою, адже є елементом системи внутрішньобанківського контролю [1], системна інтеграція якої у банки розпочалась з 2015 року з метою посилення економічної безпеки кожної окремої банківської установи та банківського сектору в цілому.

Ефективність системи комплаєнс має оцінюватись внутрішньобанківським аудитом за наступними критеріями:

- структурна та процесна інтегрованість системи комплаєнс,
- ефективність функціональної складової,
- управління комплаєнс ризиками.

Отже, система комплаєнс має бути добре розвиненою та ефективно інтегрованою структурно. Рівень комплаєнс ризиків банку надає змогу оцінити репутаційний рівень банку. Якщо рівень комплаєнс ризиків високий, та неконтрольований – гудвіл банку є практично відсутнім. Якщо ж рівень ризиків комплаєнс є низьким – гудвіл банку є високим.

Розглянемо комплаєнс системно [2], [3] тобто у взаємозв’язку його елементів. Отже, банківська інституція за своєю природою є високо-ризиковою системою, тож зобов'язана дотримуватися багатьох вимог, стандартів (норм), нормативів, згідно законодавства та етичних норм.

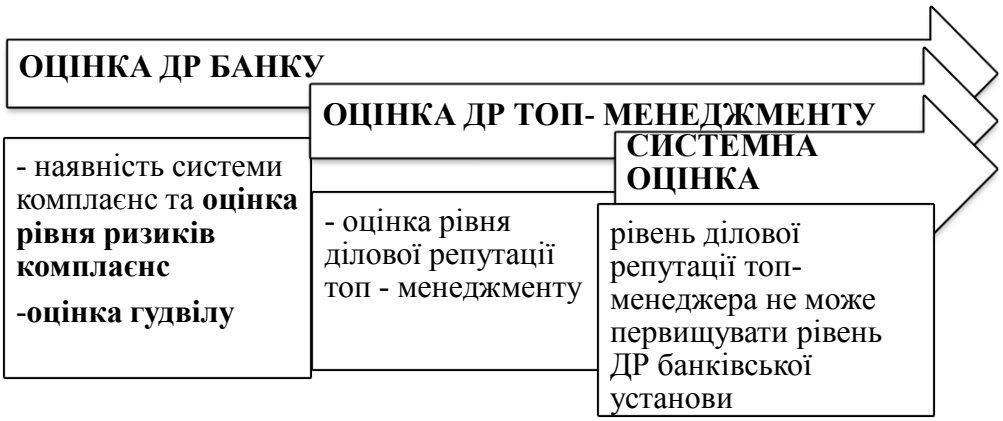


Рис. 3.5. Концепція системної оцінки

Невідповідність діяльності банку сукупності встановлених правил може спричинити незворотні наслідки як для самої кредитної організації, так і для її клієнтів і контрагентів. Запобігання подібним ситуаціям та підвищення рівня репутації банківської установи – це й є квінтесенцією функціонального навантаження системи комплаєнс.

Кардинальною відмінністю системи комплаєнс від інших елементів системи внутрішньобанківського контролю є її матеріальна - фінансова складова. Відображенням наявності/відсутності системи комплаєнс в банку виступає бухгалтерська стаття «гудвіл», що може становити додатково від 0,1% до 96% від вартості фінансової інституції. Отже за своєю природою комплаєнс є елементом економічної безпеки банківської інституції, що є вираження економічного ефекту рівня ділової репутації банківської інституції.

Отже, з метою оцінки першого елементу системної оцінки ефективності системи комплаєнс - структурна та процесна інтегрованість системи комплаєнс - автор проаналізовала досвід зарубіжних та вітчизняних банківських інституцій та удосконалено алгоритм формування системи комплаєнс в банківській установі. Тож Банк може скористатись первинною базовою моделлю поетапного створення системи комплаєнс «чотири кроки», запропонований авторкою, який схематично зображено на рисунку 3.6.

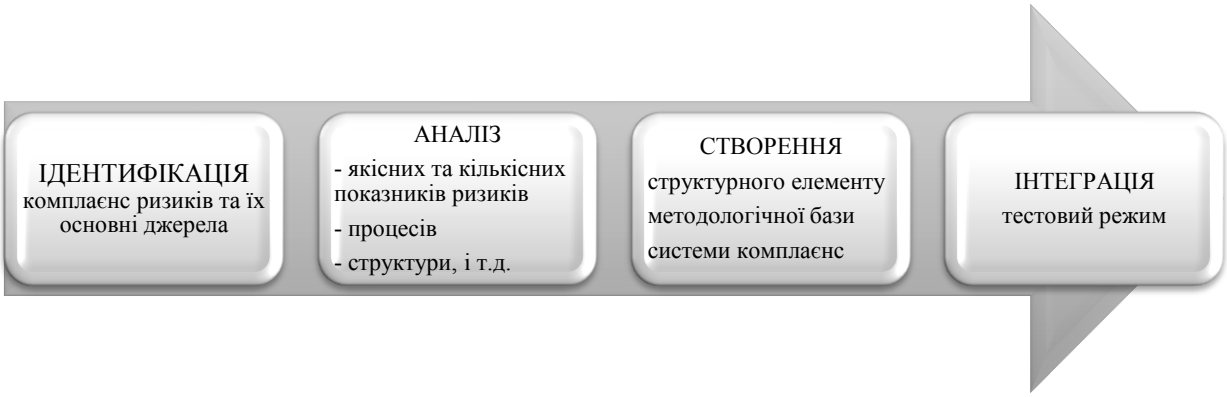


Рис. 3.6. Первинна базова модель поетапного формування системи комплаєнс в банківських інституціях «Чотири Кроки»

Банк міжнародних розрахунків, при якому в 1974 р був створений Базельський Комітет з банківського нагляду, що розробляє директиви та рекомендації, спрямовані на вдосконалення банківського регулювання і веде роботу по уніфікації вимог до фінансового регулювання в різних країнах, створив систему комплаєнс, провівши цільове об’єднання операційних та комплаєнс ризиків та підпорядкувавши відповідальну особу за комплаєнс Наглядовій Раді. В рамках системи комплаєнс Банку функціональне забезпечення внутрішнього контролю комплаєнс наступним чином:

- юридична структурна одиниця - несе відповідальність за своєчасне та правомірне тлумачення законодавчих норм, контроль за фінансовими ризиками покладено на структурний блок,
- відповідальна особа за комплаєнс банку відповідальна за створення, впровадження та перманентний моніторинг системи комплаєнс ризиків,
- структурна одиниця, що забезпечує фінансовий моніторингу банку [4], [5], [6],
- ризик менеджмент операційних ризиків (в тому числі ризиків інформаційної безпеки) може структурно підпорядковуватись відповідальній особі за комплаєнс банку,
- кадровий підрозділ банку несе відповідальність за деонтологію та підготовку тренінгового навчання разом із відповідальною за комплаєнс особою, яка безпосередньо проводить дане навчання,

- внутрішній аудит Банку є відповідальним за перевірку адекватності внутрішнього контролю системи комплаєнс, встановленого з метою забезпечення політик, планів, процедур і бізнес-цілей Банку.

Банк може створити структурний підрозділ, що підпорядковуватиметься Наглядовій Раді та окрім комплаєнс ризиків аналізуватиме також операційні ризики, або взагалі усі не фінансові ризики, розклавши їх у причинно-наслідковій послідовності, яка на сьогодні ще недостатньо описана, та потребує доопрацювання як збоку науковців та практиків так і законотворців.

Оскільки оцінка стосується процесного управління - банківська установа також має керуватися принципом циклічності задля підвищення своєї конкурентоспроможності, отже запропоновано розглянути створений на основі попередньої схеми та із врахуванням наробок науково-дослідницької діяльності, цикл розвитку системи комплаєнс в банківській інституції України, що є актуальним й динамічним елементом банку (рисунок 3.7).

Рис. 3.7. Цикл розвитку системи комплаєнс в банках

Проаналізувавши елементи системи комплаєнс, можна виділити основний, а саме: управління ризиками комплаєнс, адже згідно Приципу 10 –аутсорсинг акту Базельського Комітету «Принципи та функції системи комплаєнс» допустимо залучення аутсорсингу для вирішення окремих завдань комплаенсу, проте управління комплаєнс - ризиками має бути одним з основних напрямків

управління ризиками в банку та залишатись під внутрішньобанківським контролем топ-менеджменту банку (рис. 3.8).

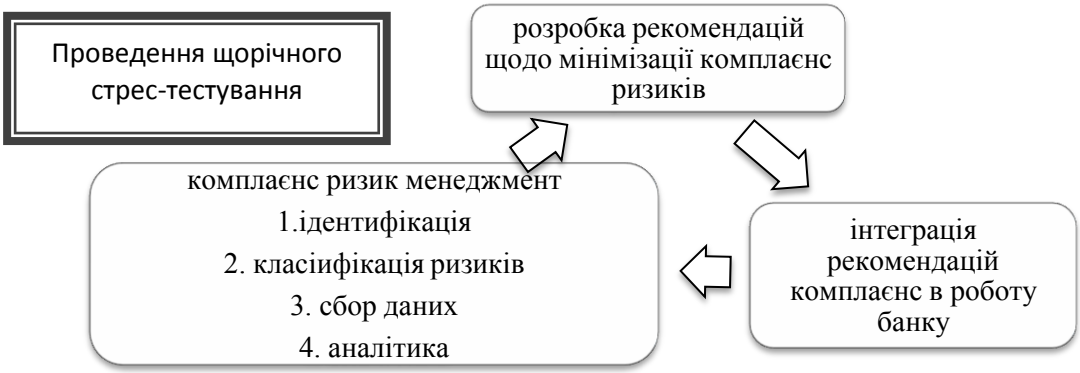


Рис. 3.8. Короткий опис основних етапів комплаєнс ризик менеджменту

Згідно актуального законодавства, Банки мають створити підрозділ, що забезпечує комплаєнс та його методологічну базу. Згідно правил міжнародного рівня та законодавчих норм України, структурно комплаєнс може бути інтегрований в банківську інституцію таким чином, щоб запобігти конфлікту інтересів. Тож структурна одиниця комплаєнс має бути інтегрована в банк залежності від його наявної структури та рівня процесного управління. З метою вдалої побудови системи комплаєнс кожен банк має проаналізувати свої процеси, якісні та кількісні показники ризиків й свою структурну модель.

Важливою складовою системи комплаєнс є функціональне навантаження останньої. Проаналізувавши міжнародні норми та законодавчі акти України стосовно комплаєнс, у таблиці 1 авторкою запропоновано квінтесенцію функціонального наповнення системи комплаєнс банківської установи.

Роль комплаєнсу в банківській справі включає виконання функцій контролю та дотримання законодавчо-нормативних актів, дотримання етичних принципів, створення та підвищення ділової репутації, захисту кадрової безпеки та фінансової безпеки.

Таблиця 3.10

Квінтесенція функціонального наповнення системи комплаєнс банківської установи

№	Функція	Зміст	Аналіз
1	Інструктаж	Консульту-вання	Відповідальна за комплаєнс особа, повинна консультувати керівництво вищої та середньої ланки стосовно дотримання актуального законодавства, правил та стандартів, в тому числі інформуючи про поточні зміни в законодавчій сфері та щодо міжнародних стандартів "найкращих практик".
2	Коорди-нація та освіта	Тренер	достатнє навчання персоналу з питань комплаєнс
3		Координатор	координує в рамках банківської установи відповіді на запити з питань комплаєнс, що надходять з/до інших банків
4		Методолог	виступає в ролі методолога: прописує/ вносить зміни до правил і стандартів, політик та процедур, та інших документів, наприклад, внутрішній корпоративний кодекс/ кодекс корпоративної етики та інших інструкцій та методик, згідно діючого законодавства України та керуючись міжнародними стандартами (в т.ч. Базельськими).
5	Ідентифі-кація, вимір та оцінка ризику комплаєнс	Ризик менеджмент	Відповідальна за комплаєнс особа, повинна визначати, ідентифікувати й оцінювати комплаєнс ризики в Банку, (в тому числі контролювати розробку нових продуктів і бізнес-процесів, створення нових видів бізнесу або відносин з клієнтами, або істотні зміни в характері цих відносин.) Якщо в банку затверджено тарифно-продуктовий комітет, відповідальна за комплаєнс особа має бути присутньою в його складі.
6	Організа-ційна безпека	Операційно – технологічни й ризик менеджмент	Відповідальна за комплаєнс особа може взяти на себе також відповідальність за управління операційними ризиками та/або створити систему управління нефінансовими ризиками Банку.
7	Репутаційна та фінансова безпека	Корпоративна етика та ризик комплаєнс фінансового моніторингу	Відповідальна особа за систему комплаєнс Банку використовує у своїй діяльності індикатори та показники KYC, та систему оцінки ризиків легалізації як клієнтів так і системи ФМ в цілому та усі інші показники, які відповідальна особа вважатиме за потрібне.
8	Репутаційна та юридично – правова безпека	Деонтологія	Відповідальна за комплаєнс особа у співпраці із юридичним підрозділом банку, повинна оцінювати відповідність дотримання чинному законодавству принципів/ стандартів та процедур банку, стежити за оновленням методологічної бази Банку і, при необхідності, надавати пропозиції та правки.
9	Моніторинг, контроль та звітність	Моніторинг та контроль	Відповідальна за комплаєнс особа повинна здійснювати періодичне стрес-тестування комплаєнс ризиків Банку та надавати результати на розгляд Наглядової Ради та Правління Банку.

№	Функція	Зміст	Аналіз
10		Звітність	Відповідальна за комплаєнс особа повинна представляти звіти з питань комплаєнс Наглядовій Раді та Правлінню Банку. Частота звітності визначається згідно діяльності та потреб Банку. Звіти повинні обов'язково включати відомості щодо управління комплаєнс ризиками за звітний період, в тому числі дії щодо їх мінімізації та превенції. Формат звітності затверджується Правлінням Банку або Наглядовою Радою.
11	План комплаєнс	Створення та затвердження Програми комплаєнс	Відповідальна за комплаєнс особа, повинна здійснювати свої функціональні обов'язки в рамках затвердженої Програми комплаєнс. Програма має включати перелік запланованих заходів, таких, як імплементація та розгляд конкретних (специфічних) політик і процедур, управління комплаєнс ризиками, тестування системи комплаєнс в Банку; навчання персоналу з питань комплаєнсу. Програма комплаєнс має бути ризик-орієнтованою та не рідше одного разу на рік переглядатись відповідальною за комплаєнс особою з метою забезпечення належного охоплення всіх бізнес процесів й адекватності структури банку та функціонального розподілу/координації ризик менеджменту.
12	Відповідальн ість та аутсорсинг	Основні функції, що не можуть бути передані на аутсорсинг	Відповідальна особа за систему комплаєнс Банку може бути куратором підрозділів, які можуть самостійно виконувати функції комплаєнс. При цьому має бути чітко прописано механізм взаємодії між Відповідальною особою та підрозділами. Комплаєнс ризики є невід’ємною функцією, що може бути виконана лише відповідальною за комплаєнс систему особою та не може бути передана жодному з підрозділів чи Правлінню

Складено автором

Підрозділи, що реалізують в банківській інституції функцію перевірки на дотримання банківською інституцією всіх діючих норм та правил регулювання банківської діяльності та відповідність усіх нормативно-методичних та стратегічних документів банку цим правилам називають «Комплаєнс-контроль» або «комплаєнс контролери».

Головним завданням комплаєнс-контролю є забезпечення створення системи внутрішнього контролю, що адекватно здійснює періодичний моніторинг, ідентифікую, оцінює і управляє ризиками, на які наражається банківська установа і насамперед комплаєнс - ризиком.

За проведеним дослідженням протягом десяти років на базі банківських установ України з різних банківських груп, з іноземним та державним капіталом та комерційних, було ідентифіковано основні види комплаєнс ризиків та систематизовано базовий каталог комплаєнс ризиків (таблиця 2) та створено графічну модель, що представляє базис для системи управління ризиками комплаєнс (рис. 3.9).

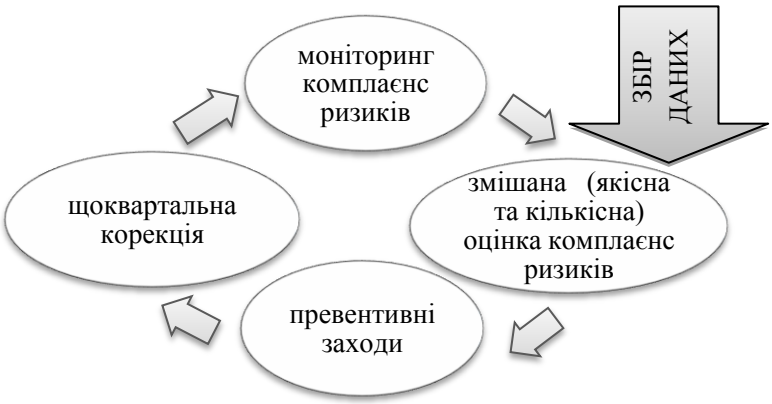


Рис. 3.9. Загальний цикл комплаєнс ризик менеджменту банку

Згідно документу Базельського комітету з банківського нагляду «Комплаєнс і функція комплаєнс в банках» під комплаєнс-ризиком розуміють ризик застосування юридичних санкцій, застосування санкцій регулюючих органів, істотного фінансового збитку, втрати репутації банком в результаті недотримання ним законів, інструкцій, правил, стандартів саморегульованих організацій або кодексів поведінки, які стосуються банківської діяльності. Даний ризик може призвести банківську установу до погіршення репутації, втрати довіри з боку регулюючих органів, партнерів, інвесторів, акціонерів, клієнтів.

На сьогодні види комплаєнс ризику практично відсутні у науковій літературі, отже автор, на основі роботи із системою комплаєнс на базі банківських установ, пропонує наступні види категорії комплаєнс ризику, а саме: регулятивний ризик, комплаєнс – ризик фінансового моніторингу, продуктовий ризик. Також комплаєнс ризик менеджмент, на думку автора, має

включати управління такими категоріями ризиків, стратегічний, політичний та геополітичний, а також репутаційний ризик.

Першим шагом на шляху до створення ефективного управління ризиками комплаєнс є проведення ефективної ідентифікації, оцінки та моніторингу комплаєнс - ризиків з ціллю їх мінімізації шляхом корегування стратегії превентивних заходів. Отже, Український банківський сектор потребує класифікації та систематизації ризиків комплаєнс, що на сьогодні відсутня. Саме тому, було розроблено та протестоване на роботі більш ніж 30-ти банківських установ на території України, каталог комплаєнс ризиків, на основі міжнародних підходів до даної категорії ризиків та створено методику проведення анкетування – збору інцидентів (загроз), що є каталізаторами реалізації комплаєнс ризиків та саму анкету - форму звітності, що наведені нижче.

Створена та запропонована автором методика кількісної, якісної та змішаної оцінки комплаєнс ризиків реалізується за допомогою наступного алгоритму:

1. Керівник визначає в результаті всебічного аналізу роботу банків, ключові структурні підрозділи, які несуть навантаження комплаєнс ризиків.

2. Керівники ключових підрозділів визначають та затверджують осіб, (згідно внутрішньобанківських процедур) що є відповідальними за заповнення форм звітності, яка має заповнюватись на періодичній основі, але не рідше ніж раз в квартал.

3. Кожен ключовий структурний підрозділ, що несе навантаження комплаєнс ризиків отримує у електронному вигляді анкету інцидентів комплаєнс, каталог комплаєнс та інсструкцію щодо заповнення анкети.

4. На основі розроблених автором каталогу комплаєнс ризиків та форми звітності та користуючись розробленою автором інструкцією визначені та затверджені особи заповнюють та надають звіти щодо інцидентів комплаєнс ризиків у банку протягом кварталу.

5. Керівник комплаєнс ризиків має консолідувати отримані дані та на основі останніх провести аналіз навантаження комплаєнс ризиків у банку.

6. Керівник комплаєнс підрозділу затверджує методологічну базу з управління ризиками комплаєнс у банку.

7. Форма звітності дає змогу визначити ймовірність настання комплаєнс ризиків, їх якісний та кількісний показник, в тому числі розмір збитків, що нанесено банку за аналітичний період (квартал). Аналітична таблиця оцінки рівня навантаження комплаєнс ризиків представлена нижче (табл. 3.12).

Таблиця 3.11

Методика розрахунку рівня навантаження комплаєнс ризиків банку

Показник	Значення	Значення об'єму навантаження
якісний	вплив на безперервність банківських процесів	Низький, середній, високий
кількісний	збитки	Так (сума)/ні
змішаний	частота	Часто, не дуже часто, рідко

Складено автором

Таблиці 3.12

Аналітична таблиця оцінки рівня навантаження комплаєнс ризиків

ЯКІСНИЙ вплив на безперервність банківських процесів	КІЛЬКІСНИЙ		Рівень навантаження ризиків
	збитки	частота	
низький	ні	рідко	незначний
низький	так	рідко	не дуже значний
низький	ні	Не дуже часто	незначний
низький	так	Не дуже часто	не дуже значний
низький	ні	часто	не дуже значний
низький	так	часто	не дуже значний
середній	ні	рідко	незначний
середній	так	рідко	не дуже значний
середній	ні	Не дуже часто	Не дуже значний
середній	так	Не дуже часто	значний
середній	ні	часто	не дуже значний
середній	так	часто	критичний
високий	ні	рідко	не дуже значний
високий	так	рідко	не дуже значний
високий	ні	Не дуже часто	не дуже значний
високий	так	Не дуже часто	значний
високий	ні	часто	значний
високий	так	часто	критичний

Складено автором

Каталог комплаєнс ризиків (таблиця 3.13) створено автором за наступним принципом - розподіллено на три основні частини: класифікація, найменування та опис ризику. Класифікація розподіляється на нефінансові ризики NFR, до категорії яких входять: CR – комплаєнс ризики AMLR- комплаєнс ризики фінансового моніторингу, PLR – продуктові ризики, PR – політичні ризики, GLR- геополітичні ризики, SR- стратегічні ризики, BRR - ризики ділової репутації.

Вперше було описано та класифіковано типи комплаєнс ризиків та комплаєнс ризиків фінансового моніторингу в банках України, оскільки останні було введено НБУ у банківський ризик менеджмент у червні 2015 року.

Таблиця 3.13

Каталог комплаєнс - ризиків

Каталог комплаєнс-ризиків			
Ризик			
Класифікація		Найменування	Опис *(приклад)*
1	2	3	4
NFR	50000	Комплаєнс-ризики	
CR	*51000*	Комплаєнс-ризик	Ризик юридичних санкцій, фінансових збитків або втрати репутації внаслідок невиконання банком вимог законодавства України, нормативно-правових актів, внутрішніх положень і правил, а також стандартів саморегулівних організацій, що застосовуються до його діяльності.
CR	51001	Неузгодженість внутрішньо-нормативних актів із законодавчими актами України	
CR	51002	Неузгодженість процесів банку із внутрішньо-правовими актами банку	
CR	51003	Адаптація "best practice" невідповідно законодавству україни	
CR	51004	Наявність розривів у процесах банку	
CR	51005	Недосконала система внутрішнього контролю	
CR	51006	Ризик внутрішньобанківських конфліктів інтересів банку	
CR	51007	Дезінтеграція (невідповідність чинним нормам) вертикальної системи менеджменту банку	
CR	51008	Ризик неадекватного корпоративного управління та деонтології	
CR	51009	Наявність неадекватного продуктового менеджменту	
CR	51010	Усі інші, схожі за типом ризики, які не ввійшли до вищенаведеного переліку	
CR	*51200*	Регулятивний ризик	Ризик недотримання вимог регулятора, що означає загрозу втрат через невиконання у щоденній роботі юридичних норм та стандартів, що встановлено

Каталог комплаєнс-ризиків			
Ризик			
Класифікація		Найменування	Опис *(приклад)*
1	2	3	4
			регулятором, а також внутрішніх нормативно – правових актів банку. Фактори, які визначають даний ризик, включають–фінансові втрати як для клієнтів, так і фінансовий збиток для банківської установи.
AMLR	52000	Ризики використання банка з ціллю легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення	
AMLR	*52100*	Клієнтські ризики	Система оцінки ризиків легалізації (відмиванням) доходів, одержаних злочинним шляхом, ризиками фінансування тероризму та фінансування розповсюдження зброї масового знищення
AMLR	52101	Ризик використання послуг банку з метою легалізації (відмиванням) доходів, одержаних злочинним шляхом, ризиками фінансування тероризму та фінансування розповсюдження зброї масового знищення	
AMLR	52102	Ризик країни (географічний), до якої належить клієнт, або з якою співпрацює	
AMLR	52103	Ризик за видом економічної діяльності	
AMLR	52104	Усі інші, схожі за типом ризики, які не ввійшли до вищенаведеного переліку	
AMLR	*52200*	Ризик порушень в частині ідентифікація клієнтів/ контрагентів банку	Проведення ідентифікації клієнта із порушеннями нормативно-правових актів, щодо проведення фінансового моніторингу в банках україни
AMLR	52201	Неповноцінне проведення ідентифікації клієнта (наприклад, несвоєчасне проведення повторної ідентифікації)	
AMLR	52202	Ризик не вивчення (не повного виявлення) групи пов'язаних осіб	
AMLR	52203	Усі інші, схожі за типом ризики, які не ввійшли до вищенаведеного переліку	
AMLR	*52300*	Ризик неадекватної системи здійснення фінансового моніторингу в банку	
AMLR	52301	Ризик порушення чи зловживання процедурою блокування операції, згідно повноважень ФМ банку	
AMLR	52302	Ризик співпраці із терористами співробітників банку	
AMLR	52303	Наявність фактів порушень законодавства у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму та фінансування розповсюдження зброї масового знищення	
AMLR	52304	Ризик легалізації доходів, шляхом схем та інших інструментів з використання банку	
AMLR	52305	Неповідомлення про операції, що мають ознаки обов'язкового фінансового моніторингу банку, або несвоєчасне повідомлення спеціально уповноважений державний орган	

Каталог комплаєнс-ризиків			
Ризик			
Класифікація		Найменування	Опис *(приклад)*
1	2	3	4
AMLR	52306	Неналежна увага до операцій, що мають ознаки внутрішнього фінансового моніторингу банку (операції, що мають заплутаний характер, тощо)	
AMLR	52307	Усі інші, схожі за типом ризики, які не ввійшли до вищенаведеного переліку	
AMLR	*52400*	Недосконала методологічна база фінансового моніторингу (далі фм) (kyc, зміни законодавства, та інше)	Порушення співробітниками законодавчих норм, стосовно фінансового моніторингу банку через відсутність внутрішньобанківського навчання, інструкцій/процедур щодо основних процесів, які можуть біти ураженими ризиками легалізації (відмивання) доходів, одержаних злочинним шляхом, ризиками фінансування тероризму та фінансування розповсюдження зброї масового знищення
AMLR	52401	Відсутність підвищення кваліфікації уповноваженої особи та співробітників банку, що задіяні в процесі фм банку	
AMLR	52402	Відсутність/ недосконалість системи контролю фм	
AMLR	52403	Відсутність політики/ недотримання принципу «знай свого клієнта»;	
AMLR	52404	Ненадання/ несвоєчасне надання звітності фм	
AMLR	52405	Ризик неналежного зберігання відомостей щодо клієнта (порушення термінів зберігання, і т.д.)	
AMLR	52406	Відсутність належного досвіду та навичок персоналу банку в оперативній та ефективній протидії легалізації доходів, одержаних злочинним шляхом і фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення, а також іншої діяльності, яка відповідно до законодавства країни здійснюється протиправно контрагентами, клієнтами або персоналом банку	
AMLR	52407	Усі інші, схожі за типом ризики, які не ввійшли до вищенаведеного переліку	
PLR	*53000*	Ризик продуктовий	Ризик зниження конкурентоспроможності продуктового ряду банку, у зв’язку із масивом внутрішньобанківських причин
PLR	53001	Низька якість продукту порівняно з продуктами, які пропонуються іншими банківськими установами	
PLR	53002	Ризик невідповідності співвідношення якості та ціни продукту	
PLR	53003	Ризик нестабільності продукту, відсутності динамічності та новизни продукту	
PLR	53004	Неефективний продуктовий менеджмент, що не виконує (виконує не в повній мірі) функцію розробки нових продуктів та комплексних пропозицій з метою підвищення конкурентоспроможності та збільшення прибутковості	

Каталог комплаєнс-ризиків			
Ризик			
Класифікація		Найменування	Опис *(приклад)*
1	2	3	4
PLR	53005	Ризик невідповідності формату банку продуктовій лінійці банку (продуктова лінійка має відповідати видам діяльності банку та забезпечувати ринкові потреби у відповідності до масштабів діяльності банківської установи)	
PR	54000	Політичний ризик	Ризик виникнення несприятливих умов в банківському секторі україни через політично нестабільну ситуацію
GPR	54100	Геополітичний ризик	Ризик виникнення економічно-несприятливих умов в регіональному масштабі україни через політично нестабільну ситуацію
SR	55000	Стратегічний ризик	Наявний або потенційний ризик для надходжень та капіталу, який виникає через неправильні управлінські рішення, неналежну реалізацію рішень і неадекватне реагування на зміни в бізнес-середовищі. Цей ризик виникає внаслідок несумісності: стратегічних цілей банку; бізнес-стратегій, розроблених для досягнення цих цілей; ресурсів, задіяних для досягнення цих цілей; якості їх реалізації.
BRR	56000	Ризик ділової репутації	Наявний або потенційний ризик для надходжень та капіталу, який виникає через несприятливе сприйняття іміджу фінансової установи клієнтами, контрагентами, акціонерами (учасниками) або органами нагляду.
BRR	*56100*	Ризик репутації який виникає внаслідок внутрішніх процесів банку	
BRR	56101	Безвідповідальні дії працівників, а саме недотримання норм ділового спілкування, порушення деонтології банку - принципів професійної етики, порушення зобов'язань за договором(рами) перед контрагентами, клієнтами	
BRR	56102	Розголошення комерційної таємниці	
		Неефективне управління різними видами ризиків, які притаманні банківській установі та здатні нанести шкоду його діловій репутації та діловій репутації його топ - менеджменту	
BRR	56103	Звільнення ключових співробітників	
BRR	56104	Порушення банком законодавства	
BRR	56105	Свідомі дії співробітників, що підривають репутацію банку	
BRR	*56200*	Ризик репутації який виникає внаслідок зовнішніх чинників	
BRR	56201	Висловлювання чиновників на адресу банку	
BRR	56202	Неправомірні дії конкурентів, (демпінг, тощо)	
BRR	56203	Несприятлива ситуація в банківському секторі	
BRR	56204	Розповсюдження негативної інформації стосовно банківської установи, її топ-менеджменту та будь-яких її службовців, а також дочірніх структур, тощо	
BRR	56205	Несанкціоновані публікації в змі та інтернет, чорний pr	
BRR	56206	Зовнішня інформація щодо недосконалого менеджменту банку/ невдоволеність клієнтів, що надходить з будь-яких джерел	

Каталог комплаєнс-ризиків			
Ризик			
Класифікація		Найменування	Опис *(приклад)*
1	2	3	4
BRR	56207	Виникнення конфлікту інтересів у банківської інституції з зацікавленими сторонами, як засновники, контрагенти, клієнти та ін;	
BRR	56208	Інші, схожі за типов ризики, що не увійшли до списку	

Складено автором

Після затвердження даного каталогу, банк має розробити та затвердити форму звітності (табл. 3.14), яку мають заповнювати особи, які є власниками бізнес процесів банку, при чому власники не лише критичних бізнес процесів, що є дуже важливим аспектом.

Базуючись на міжнародному досвіді та власному практичному досвіді, що квартальний аналіз дає можливість побудувати матрицю ризиків комплаєнс банку та створити систему контролю за ними.

В рамках апробації даної методики більш ніж сорок банків України використовують дану методику.

Згідно з методикою оцінки ризиків комплаєнс, що розроблено автором, аналіз комплаєнс ризиків банку потрібно проводити не рідше, ніж один раз у щоквартальний термін.

Банк має вирішити які з вищенаведених ризиків з каталогу ризиків комплаєнс є для нього найвагомішими у зв’язку із специфікою його діяльності та аналізувати їх згідно своїх шкал критичності.

Форма звітності представляє собою анкету інцидентів реалізованих комплаєнс ризиків, що враховує кількісні та якісні показники останніх.

Заповнення даної форми проводиться за допомогою інформації з каталогу комплаєнс ризиків та значно спрощує роботу із даною формою.

Зразок заповнення форми звітності та інформація, яка вноситься до форми представлено на наступній сторінці.

Провівши системний якісний та кількісний аналіз ризиків, процесної та структурної моделі, функціональної складової направленості банківської

діяльності та заклавши ефект, який бажає отримати конкретна банківська установа, можна отримати оцінку ефективності системи комплаєнс саме даної банківської інституції, як елементу концептуальної системної оцінки ділової репутації як банку так і його топ-менеджменту.

Таблиця 3.14

Форма звітності

Анкета інцидентів реалізованих комплаєнс-ризиків				
ПІБ Відповідальної особи				
Підрозділ				
Код ризику (із каталогу комплаєнс ризиків)	Частота (кількість випадків за звітний період)	Вплив на безперервність банківських процесів	Збитки (грн.)	Коментар

Варіант відповіді

Показник	Частота	Вплив на безперервність банківських процесів	Збитки
Якісний	*Частота*	*Низький*	*Так*
	Не дуже часто	*Середній*	*Ні*
	Рідко	*Критичний*	
Кількісний	*або кількість випадків за звітний період*	-	*Грошовий еквівалент (грн.)*

Складено автором

З метою системної оцінки рівня ділової репутації, необхідно вивчити наступні складові системи банківської установи, а саме:

1. Склад власників. Наявність серед акціонерів банку великих компаній, що мають економічний та політичний вплив, за інших рівних умов позитивно позначається на його репутації. У разі ж зміни власників оцінка вірогідних наслідків цього може бути різною.

2. Входження банку у фінансово-промислову групу або холдинг. У процесі аналізу до уваги беруть як успішність та масштабність того або іншого холдингу, так і позиціонування в ньому банку.

3. Стабільність чи нестабільність топ-менеджменту. За інших рівних, умов звільнення (за відсутності адекватних причин) перших осіб і, тим більше, цілої команди топ-менеджерів, скандали між керівниками банківської установи чи її власниками є, звісно, негативним чинником, що посилює ризик погіршення репутації.

4. Загальні тенденції в розвитку банку. Увагу акцентують на ринкових позиціях банку, опануванні ним нових ринків, впровадженні перспективних програм, розширенні клієнтської бази, розвитку філійної мережі тощо.

5. Рівень аудиту, наявність рейтингів. За інших рівних умов співпраця банку з авторитетним аудитором, надання звітності, що відповідає міжнародним стандартам, присвоєння банківській установі високих рейтингів, безумовно, позитивно позначається на її репутації.

6. Інформаційна відкритість, наявність зрозумілої стратегії розвитку. Інформаційна прозорість банку виражається в обсязі та якості відомостей, що пропонуються зацікавленим особам, пресі тощо.

7. Наявність проблем у стосунках із державними і податковими органами.

Як відомо, репутація складається лише на основі минулої діяльності, та фактів й критеріїв оцінки ризиків комплаєнс, ділової репутації топ-менеджменту банку, тож системність підходу оцінки ділової репутації топ – менеджменту можна окреслити у створенні на основі законодавчих критеріїв системної методики оцінки топ – менеджменту банку та динамічному контролі останньої шляхом управління ризиком репутації, з метою не допущення її погіршення та за результатами оцінки комплаєнс ризиків й вироблених на її основі заходів (в тому числі превентивних) проведення своєчасної корекції репутації топ - менеджменту та її нарощування.

Новизна даного дослідження полягає у створенні методики оцінки топ – менеджменту банку на основі анкетування, за яким було проведено апробацію

на прикладі банків України, що показало дієвість та високу ефективність новітньої методики.

Дана методика надає також можливість оцінки рівня ділової репутації топ-менеджменту та опосередкованої оцінки рівня ризиків репутації банку, комплаєнс ризиків або гудвілу банку, що виявляє системність методики оцінки рівня ділової репутації топ- менеджменту.

На основі проведених досліджень системи внутрішньобанківського контролю економічної безпеки, а саме системи фінансового моніторингу банку було розроблено та проведено програму навчання в Державній Службі Фінансового Моніторингу України, яка була затверджена Національним Банком України, а саме: «Інститути фінансово-майнового контролю конфлікту інтересів національних публічних діячів: майнові декларації, їхня структура, облік, розкриття (оприлюднення) та перевірка», «Порядок реєстрації та передачі інформації про фінансові операції, що підлягають фінансовому моніторингу. Форми обліку та подання інформації, пов'язаної із здійсненням фінансового моніторингу. Порядок виправлення помилок в повідомленнях про фінансову операцію.», «Порядок подання інформації Держфінмоніторингу та повідомлення правоохоронним органам про фінансові операції, щодо яких є мотивовані підозри, що вони пов'язані з легалізацією (відмиванням) доходів, одержаних злочинним шляхом, або якщо вони пов'язані, стосуються чи призначені для фінансування тероризму, розповсюдження зброї масового знищення. Вимоги щодо запобігання розголошенню інформації, яка надається Держфінмоніторингу, іншої інформації з питань фінансового моніторингу, у тому числі про факт її подання.»

Список використаних джерел:

1. *Статут Комплаєнс BIS 9 травня 2005; остання редакція 8 січня 2007 http://www.bis.org/about/compliancecharter.pdf (дата доступу 04.11.15)*
2. *Принципы, направленные на улучшение корпоративного управления, октябрь 2010 г. На англ. яз. "Principles for enhancing corporate governance".*
3. *Основные принципы эффективного банковского надзора, сентябрь 2012 г. На англ. яз. "Core Principles for Effective Banking Supervision". Источник информации:http://www.bis.org/publ/bcbs230.pdf*

4. *Управління ризиками, пов'язаними з відмиванням грошей і фінансуванням тероризму. Базельський комітет з питань банківського нагляду - січень 2014 року.http://www.bis.org/publ/bcbs275.pdf (дата доступу 20.09.15)*
5. *Рекомендації ФАТФ - міжнародні стандарти по боротьбі з відмиванням грошей і фінансуванням тероризму та зброї. Лютий 2012ю Оновлено в жовтні 2015.http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf (дата доступу 14.11.15)*
6. *Консолідована Політика Знай Свого Клієнта (ЗСК) Управління ризиками - Остаточний документ - жовтень 2004ю Базельський комітет з управління ризиками банківського нагляду консолідованої ЗСК. http://www.bis.org/publ/bcbs110.htm (дата доступу 02.11.15)*

3.4. ЕФЕКТИВНА РЕАЛІЗАЦІЯ ІНТЕЛЕКТУАЛЬНО – ТРУДОВОГО ПОТЕНЦІАЛУ ЯК РУШІЙНА СИЛА ІННОВАЦІЙНОГО РОЗВИТКУ ТА БЕЗПЕКИ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

ГУМЕНЮК ОЛЕКСАНДРА СЕРГІЇВНА *к.е.н, доцент,*
Східноєвропейський університет
економіки і менеджменту

В умовах глобальної конкуренції стійке зростання національної економіки та її безпека неможливі без активізації інноваційної діяльності. Досвід більшості країн-лідерів світової економіки засвідчує, що їхній успішний розвиток значною мірою визначається спроможністю створювати та впроваджувати інновації. При цьому важливим чинником інноваційного розвитку їх економіки в першу чергу є ефективне використання внутрішніх ресурсних можливостей з одночасним балансуванням зовнішніх залежностей. Тривалі негативні тенденції економічного розвитку України зумовлені незадовільною реалізацією задекларованих інноваційних цілей. Основними причинами такого стану є низька ефективність використання наявного потенціалу економіки країни, військові дії, корупція та економічні злочини. Це загострює потребу пошуку шляхів дієвої державної політики, спрямованої на мобілізацію, нагромадження й відтворення внутрішніх ресурсних можливостей економіки, зокрема інтелектуально-трудового потенціалу, з метою підвищення конкурентоспроможності України, забезпечення економічної безпеки та покращення суспільного добробуту.

Дослідження теоретико-прикладних засад реалізації інтелектуально-трудового потенціалу інноваційного розвитку національної економіки має відбуватись з посиланням на досягнення світової та вітчизняної науки. Слід відзначити праці таких зарубіжних та вітчизняних вчених, як Л. Канторович, М.Кондратьєв, Г. Менш, М. Познер, М. Портер, А. Сміт, К. Фрімен, Й. Шумпетер, Ю. Яковець та В.Антонюк, Ю.Бажал, О.Білорус, Л.Гальперіна, В.Геєць, А.Дука, Я.Жаліло, С.Захарін, Т.Затонацька, В.Захарченко, А.Колот, Е.Лібанова, Д.Лук’яненко, Б.Маліцький, В.Микитенко, І.Михасюк, О.Новікова,

В.Онікієнко, І.Петрова, М.Семикіна, В.Семиноженко, В.Соловйов, А.Чухно, Н.Чухрай, І.Ящишина та ін. Проте, незважаючи на ґрунтовні напрацювання багатьох учених, комплексного дослідження сутності та шляхів реалізації інтелектуально-трудового потенціалу інноваційного розвитку національної економіки у вітчизняній науковій літературі не простежується. Тому метою статті є пошук прогресивних підходів щодо реалізації інтелектуально-трудового потенціалу інноваційного розвитку економіки України.

Якісні дослідження ендогенного потенціалу інноваційного розвитку (ЕПІР) національної економіки багато в чому обмежуються наявною інформаційною базою. Ендогенний потенціал інноваційного розвитку це комплексна категорія й оцінювати її можна з використанням широкого набору показників. Разом з тим, більшість з них відображають суто кількісний бік інноваційної діяльності і змоделювати їх трансформацію в якісні результати важко. Водночас, існує безліч специфічних процесів і явищ у сфері інноваційної активності та векторності інноваційного розвитку економіки України, що потребують специфічних знань. Особливо це стосується використання інтелектуально-трудової компоненти, проблемність чого часто криється в суто ментально-психологічній площині. Принципи переходу до сучасного інформаційного суспільства змушують шукати нові грані можливостей діяльності людини, яка через свої потенційні характеристики здатна здійснювати значно більший вплив на економічний розвиток, аніж вона того очікує.

Для України в силу її прагнення якісного переходу до інформаційного суспільства з метою посісти заслужене місце з-поміж розвинених країн питання людського чинника загострюється з особливою силою. Причиною цьому є доволі позитивна ретроспективна оцінка інтелектуально-трудових можливостей українського народу, які виражались як у приватному господарюванні, так і здатності генерувати ідеї, що здійснювали переворот у загальних світоглядних засадах людства. Практика засвідчує, що доволі багато вихідців-емігрантів з України у новій країні зі сприятливими умовами ставали видатними вченими, успішними особистостями, чого б вони не могли досягти на батьківщині

(наприклад, Нобелівські лауреати – вихідці з України: Р. Гоффман, П. Капиця, І. Мечніков, С. Кузнець та ін.) [3, с.480]. За роки незалежності в складних макроекономічних умовах багато громадян України також доводили свої високі інтелектуальні здібності, що проявлялись навіть у несприятливому середовищі. Таким чином, є цілком закономірні підстави говорити про сформований високий інтелектуально-трудовий потенціал населення України, який щоправда не слід переоцінювати в силу помітних ціннісних деформацій та низької самооцінки вартості робочої сили.

Водночас, на наше переконання, в складних умовах економічного розвитку України та потреби ефективної реалізації її ендогенного потенціалу саме інтелектуально-трудова компонента повинна бути рушієм інноваційних змін, у тому числі з урахуванням вимог інформаційного суспільства. Це вимагає підвищення ефективності її реалізації, фактичним підтвердженням чого були і результати експертного опитування. Згідно них, дана компонента ендогенного потенціалу оцінюється у використанні лише на 4,2 бали (з максимальних 10), що є однією з найнижчих оцінок з-поміж усіх компонент. Окрім того, 22,5% експертів функціональну роль рушія інноваційних змін відводять інтелектуально-трудовому потенціалу, хоча це й дещо менше, аніж прихильників фінансової компоненти – 25,0%. Проте остання відзначається значною залежністю від зовнішніх впливів. Через те є всі підстави говорити, що саме інтелектуально-трудовий потенціал має бути пріоритетом в інноваційних змінах національної економіки через процеси його мобілізації, нагромадження і відтворення.

Виходячи з пріоритетів інноваційного розвитку України, зокрема через використання ендогенного потенціалу її економіки з метою підтримки наукоємного виробництва, слід окреслити основні заходи політики держави з оптимізації позитивного впливу інтелектуально-трудового потенціалу на ситуацію в країні. Такі заходи повинні розподілятись за різними сегментами:

– спрямовані на осіб, що навчаються – з метою формування інноваційної культури суспільства, потреби творчості, креативності, інноваційної діяльності

як способу самореалізації та можливості покращення умов життя інших людей ;

– спрямовані на економічно активне населення у відносно молодих вікових межах, що здатні до навчання і відзначаються інноваційною активністю;

– спрямовані на економічно активне населення у вікових межах старшого (передпенсійного) віку, що володіють достатнім досвідом та можуть його передати через міжпоколінні професійні знаннєві трансферти, в тому числі щодо інноваційної діяльності;

– спрямовані на підприємців, особливо малих форм бізнесу, що здатні генерувати ідеї, швидко орієнтуються в бізнес-середовищі та очікують цільової підтримки у реалізації проектів;

– спрямовані на працівників наукової й освітньої сфер, що володіють необхідним методичним інструментарієм та за наявності відповідного матеріально-технічного забезпечення здатні ініціювати процеси інноваційної діяльності у співпраці з іншими структурами (особливо суб’єктами господарювання);

– спрямовані на трудових мігрантів з України, представників діаспори, що відзначаються високими інтелектуальними здібностями, мають ресурсні можливості ведення бізнесу в наукоємних видах економічної діяльності та за умов цільової підтримки готові повернутись в Україну (селективний підхід стимулювання рееміграції);

– спрямовані на все суспільство з метою формування його інноваційної культури, ставлення з повагою до осіб, що займаються інноваційною діяльністю (формування інноваційної культури регламентовано чинним законодавством) [6].

Важливим результуючим вимірником забезпечення рушійності з боку інтелектуально-трудового потенціалу інноваційних змін є наявність у країні інтелектуальної еліти, причому не пасивної та підвладної з вимушеним реагуванням на політичні «замовлення», а авторитетної в суспільстві, спроможної спричиняти потужний вплив на суспільну думку через науково обґрунтовані твердження і, що головне, результативної в генеруванні нових

ідей. Такі ідеї не повинні обмежуватись лише тими, що стосуються пріоритетів інноваційного розвитку національної економіки, але й комплексно торкатись усіх сфер суспільного життя з націленістю на покращення якості життя людини.

Формуванню інтелектуальної еліти повинно передувати явище так званої інтелектуальної монополії. Це єдиний вид монополії у світовому бізнесі, що визначається та заохочується як на національному, так і на міжнародному рівнях, оскільки створення максимально сприятливих умов для розвитку інтелектуальної еліти в країні надає можливості розвитку інноваційної економіки [13, с. 85]. У сучасних умовах віртуалізації інформаційного простору не обов'язковою є концентрація інтелектуальної еліти в обмежених просторово-часових координатах з одержанням переваг синергетичних ефектів соціального капіталу. Розосередження представників-інтелектуалів дасть змогу локалізувати наукові осередки з можливістю досліджень проблем територіального характеру, що потребують урахування місцевої специфіки, а також сформувати своєрідне конкурентне середовище наукових шкіл, що буде додатковим мотиватором якісних наукових досліджень.

Методологічною основою обґрунтування рушійності інтелектуально-трудового потенціалу населення України в контексті забезпечення інноваційних змін є положення соціально-психологічної теорії інноваційного розвитку, яка розглядає людський капітал як ключовий фактор економічного розвитку взагалі. Прикладним аспектом пріоритетів мобілізації, нагромадження та відтворення потенціалу мають бути проблемні прояви сфери соціально-трудових відносин та перспективи їх розвитку (в різночасовому розрізі) з націленістю на створення сприятливих передумов використання потенційних характеристик населення. Проблемні прояви детермінують відмінності в пріоритетах покращення використання інтелектуально-трудового потенціалу зайнятого населення задля оптимізації стимулюючого його впливу на інноваційний розвиток національної економіки (табл. 1).

Водночас основним зрізом підвищення ефективності використання

інтелектуально-трудових можливостей населення, зайнятого в економіці України, наразі постає їх відтворення в силу вже тривалих процесів інтелектуальних, демографічних (у т.ч. міграційних) втрат, втрат людського й соціального капіталу тощо (щодо соціального капіталу особливо деструктивує пониження суспільної довіри, у тому числі до органів державної влади). Якщо поточні тенденції демотивації продуктивної трудової діяльності будуть продовжувати зберігатись, а якісні параметри підготовки системою освіти фахівців і робітників не відповідатимуть новим потребам інноваційної економіки, то говорити про ефективне використання інтелектуально-трудового потенціалу як рушія інноваційних змін стане недоцільно, оскільки такий потенціал буде втрачати свої сильні сторони. Деградаційні процеси будуть відзначатись подальшими схильностями населення до максимізації доходу з докладанням найменших зусиль, формального виконання посадових зобов'язань, масовими явищами так званої психологічної плинності кадрів (видимість зайнятості на робочому місці) тощо.

Сформульовані в табл. 3.15 цілі (стратегічні й поточні) в значній мірі корелюють зі стратегічними цілями інноваційного розвитку економіки України.

Таблиця 3.15

Специфіка реалізації інтелектуально-трудового потенціалу зайнятого населення в системі інноваційного розвитку національної економіки*

№ з/п	Характе-ристики	Мобілізація	Нагромадження	Відтворення
1	Загальна сутність	Максимальне кількісне залучення економічно активного населення до інноваційної діяльності з формуванням відповідного конкурентного середовища.	Тимчасове кількісно-якісне збільшення інноваційно активного населення з поступовою підготовкою нових поколінь, здатних посилювати набутий досвід через міжпоколінні знаннєві трансферти.	Приведення кількісно-якісних характеристик економічно активного населення до визначених еталонних значень «радянського періоду» з високим рівнем розвитку інженерних спеціалізацій, фахівців медичного та ін. напрямів, патріотизмом праці.
2	Основні проблеми	Тіньова зайнятість. Добровільне безробіття.	Малопрестижність науково-дослідної діяльності. Слабо налагоджена	Значна зміна освітньо-кваліфікаційної структури випускників

№ з/п	Характе-ристики	Мобілізація	Нагромадження	Відтворення
		Еміграція.	система міжпоколінних професійних знаннєвих трансфертів.	закладів освіти. Непослідовна соціальна політика держави.
3	Стратегічна ціль	Трансформація кількісного залучення населення до інноваційних процесів в якісні результати інноваційної діяльності.	Підвищення якісних результатів інноваційної діяльності з їх впровад-женням у сприятливі періоди (спаду – як каталізатора покращення, росту – як способу одержання кращих ефектів).	Оптимізація освітньо-кваліфікаційної структури населення до перспективної потреби інноваційної економіки.
4	Поточні цілі	Детінізація зайнятості. Формування мотиваційного середовища продуктивної інноваційної діяльності. Формування загальної інноваційної культури населення через «вимушене» залучення до побутового споживання інноваційних технологій.	Посилення наукової складової освітнього процесу (починаючи з закладів дошкільного типу) задля підготовки нової генерації фахівців.	Цільове фінансування якісної підготовки спеціалізованих фахівців (робітників). Цільова підтримка інноваційних проектів (система стартапів, краудфандингу). Ефективне підвищення кваліфікації з вивченням нових технологій у професії, мов.

**Розроблено автором*

Обґрунтуємо більш конкретно найбільш нагальні у досягненні з них, які дозволять:

– мобілізувати трудопотенційні можливості населення, сформовані у попередні роки, з націленістю на інноваційну діяльність як форму якісного їх використання з відображенням у результатах праці й одержанням не лише економічних, але й соціальних, екологічних, науково-технічних та інших ефектів;

– розпочати процеси нагромадження інтелектуально-трудового потенціалу як протилежного процесу до помітних трудопотенційних втрат через деінтелектуалізацію населення, погіршення демопоказників, активні еміграційні процеси; у подальшому нагромадження інтелектуально-трудового

потенціалу мають бути максимально мобілізовані задля забезпечення інноваційного прориву економіки України;

– розпочати процеси відтворення трудопотенційних можливостей населення з відновленням традицій господарювання, ремісництва (для розвитку малого бізнесу), міжпоколінних династій фахівців і робітників, у тому числі в професіях інноваційного характеру.

У першу чергу постає необхідність налагодження розвиненої системи міжпоколінних знаннєвих трансфертів професійного характеру. Мається на увазі передача досвіду економічно активного населення, яке переходить у соціальний статус пенсіонерів та молоді, що здобула освіту та розпочинає трудову діяльність. Тобто орієнтовно це 30-40 років. Рівень розвитку системи міжпоколінних знаннєвих трансфертів засвідчує так звана міжпоколінна мобільність, що дає змогу співставити професійний шлях попереднього покоління у визначених вікових межах до сучасного в кращих, удосконалених умовах зі здатністю використовувати нові можливості трудової діяльності та реалізації інтелектуально-трудового потенціалу.

Вважаємо, що наразі називати період розвитку України інформаційним суспільством є не правильним, адже воно набуває деформованих ознак. У гонитві за світовими стандартами та прагненням представлення в статистичній звітності достатніх результатів інноваційної діяльності суб’єктів господарювання, наукових й освітніх установ, маємо ситуацію неорганічного переходу до інформаційного суспільства, коли насправді його ознаки концентровані в окремих просторових утвореннях зі значною міжрегіональною дивергенцією за показниками інноваційного розвитку.

Основою формування системи знань у межах професійної групи одного покоління є відповідні середовищні умови (як поточні умови життєдіяльності та праці, що поступово змінюються) та інституціональне середовище (як більш стійкі прояви способу життя суспільства, норм поведінки, трудової активності тощо). Такі умови сьогодні особливо динамічно змінюються, що частково руйнує нагальну потребу прямих міжпоколінних знаннєвих трансфертів у силу

зовсім відмінних пріоритетів суспільного розвитку. Зокрема виникають нові види економічної діяльності, які потребують абсолютно нових знань. Проте в будь-якому випадку знаннєві основи попередніх поколінь формують цілісний алгоритм суспільних знань, що можуть бути адаптовані до різних сфер життєдіяльності людини, в тому числі економічної.

Якщо ми говоримо про інноваційний розвиток національної економіки, де рушієм таких процесів має постати інтелектуально-трудовий потенціал її зайнятого населення, то зруйнована наразі система міжпоколінних знаннєвих трансфертів професійного характеру прямо позначається на результатах інноваційної діяльності. Та когорта високопрофесійних фахівців здебільшого інженерної спеціалізації, космічної, авіабудівничої сфер, радіоелектроніки й інших, що наразі залишилась, за умов відсутності продуманої структурної політики (структура національної економіки наразі формується стихійно з орієнтиром на сировинні можливості країни) та при колосальному зносі основних фондів не має змоги якісно передати свої в першу чергу прикладні навики молодим фахівцям. Руйнація матеріально-технічної бази стратегічних колись сфер машинобудівної, переробної промисловості робить відповідні види економічної діяльності непривабливими для зайнятості в очах випускників загальноосвітніх навчальних закладів. Це помітно деформує систему передачі знань професійного характеру та не дозволяє простежувати хоч якусь міжпоколінну мобільність населення з системним нагромадженням таких знань.

Система міжпоколінних знаннєвих трансфертів професійного характеру повинна проявлятись через способи передачі знань. Найбільш ефективними є безпосередні контакти з молодими фахівцями (робітниками) у виробничому середовищі. За таких умов підвищується значимість корпоративних цінностей із розвитком системи підвищення кваліфікації кадрів та переважним залученням штатних працівників. Це означає, що у межах бізнес-структур повинні функціонувати підрозділи стажування, тренінгового навчання тощо через організовану передачу знань провідних фахівців молодим та потенційним працівникам, які через їх акумуляцію зможуть удосконалювати способи

досягнення результатів праці, в тому числі з посиленням їх інноваційного характеру.

Закономірним є висновок про потребу такого способу передачі знань, як викладацька діяльність. Реальність залучення фахівців-практиків пріоритетних для інноваційного розвитку видів економічної діяльності в освітній процес ускладнена численними деформаціями в національній освітній системі, що прямо відображаються на якості освітньої підготовки (особливо в частині помітного розриву теоретичних знань та прикладних навиків у виробничих умовах). Проте така необхідність наразі є доволі високою й ініціатором даних процесів мають виступати самі заклади освіти з метою посилення своїх конкурентних позицій на ринку через інструментарій маркетингу освітніх послуг. Це означає, що викладацька діяльність успішних практиків з навиками інноваційної діяльності має стати стимулом вступу і навчання випускників загальноосвітніх закладів до відповідного ВУЗу.

У системі міжпоколінних професійних трансфертів також свою нішу займає науково-видавнича діяльність фахівців-практиків. Сьогодні вона набула комерційного характеру та особливо популярна в сферах підприємництва, маркетингу, управління персоналом. Водночас така форма передачі знань є важливою для формування схильностей у суспільстві до здобуття відповідних професій.

Вважаємо, що наразі головними способами трансферу знань мають бути безпосередні контакти з молодими фахівцями у виробничому середовищі, а також побутове спілкування. Через побутове спілкування можливим є формування сімейних династій-професіоналів, які б будувались не на інтересах володіння й нагромадження власності чи великого бізнесу, а в ремеслі досягнення результатів праці задля виробництва якісної продукції, здатної задовольняти потреби суспільства та покращувати якісні характеристики його життя.

Підсумовуючи пріоритети розвитку системи міжпоколінних професійних знаннєвих трансфертів, для забезпечення інноваційного розвитку економіки

України наразі важливим постає недопущення втрати прикладних навиків фахівців тих сфер, що були провідними в радянський період та перші роки державної незалежності. У сучасних умовах переходу країни до інформаційного суспільства такі сфери не втрачають своєї актуальності, а навпаки є дуже важливими до розвитку в силу незадовільного рівня інноваційності в економіці України. Тому фахівців і робітників тих професій, що важливі для посилення інноваційної діяльності в сучасних сферах, слід залучати в освітній процес, а також до навчання (стажування) і підвищення кваліфікації молодого персоналу безпосередньо у виробничих умовах. Для цього не слід обмежуватись особами економічно активного населення. Важливою є включеність і осіб пенсійного віку, що за станом здоров'я спроможні і мають мотивацію передавати свої знання й навики наступним поколінням.

Забезпечення рушійності використання інтелектуально-трудового потенціалу задля інноваційного розвитку економіки України окрім системи міжпоколінної передачі знань потребує відтворення тих трудопотенційних можливостей населення, які вже сформовані, проте не мають змоги проявлятись у результатах інноваційної діяльності в зв'язку з браком ресурсного оснащення. Тому серед важливих пріоритетів посилення ролі інтелектуально-трудових можливостей населення в частині їх відтворення постає необхідність цільової підтримки інноваційних проектів. Форм такої підтримки світовий досвід засвідчує достатньо. У вітчизняних реаліях найбільш часто декларується програмно-цільове фінансування, проте фактичність виділення коштів на реалізацію таких програм є вкрай низькою, що змушує відходити від пріоритетності даного варіанту стимулювання реалізації інтелектуально-трудового потенціалу з продуктивною інноваційною діяльністю. Враховуючи те, що за рахунок державного бюджету чи державних позабюджетних фондів допомога скерована на пріоритетні, стратегічно важливі для держави напрями досліджень (переважно фундаментального характеру, а також інфраструктурні проекти, закупівлю передових іноземних технологій,

ліцензій і патентів, участь у міжнародних науково-технічних програмах), незадовільне використання таких коштів є свідченням вкрай неефективної державної інноваційної політики, яка тим більше не враховує ендогенні потенційні можливості національної економіки [8].

Формування схильностей населення до інноваційної діяльності в поки недосконалому конкурентному середовищі також виглядає ускладненим на рівні бізнесу великих форм власності, зокрема через залучення інвестиційних коштів в інноваційні бізнес-проекти. Такі проекти є доволі ресурсно-затратні та в мінливому бізнес-середовищі спрогнозувати їх окупність вкрай складно. Відтак це демотивує підприємців до їх впровадження.

Звичайно, цільова підтримка інноваційної діяльності на рівні держави (у т.ч. через бюджетне фінансування) та великих підприємств важлива і необхідна. Проте згідно проблемних реалій інноваційної активності населення України, що в більшості випадків вкрай неефективно використовує свої трудопотенційні можливості, видається ефективнішим пошук більш прогресивних форм підтримки інноваційних проектів, які можуть бути ініційовані окремими фізичними особами (особливо молоддю). Тому вважаємо, що в Україні сьогодні слід активізовувати цільову підтримку інноваційних проектів через систему стартапів і краудфандингу. Їх практична вигідність полягає в тому, що вони стимулюють у першу чергу розвиток малого і середнього бізнесу, які відіграють величезну роль у посиленні конкурентного середовища, необхідного для стимулювання інноваційного розвитку з боку суб’єктів господарювання.

Система стартапів і краудфандингу є поширеною в світі практикою фінансування ідей підприємців-представників малого і середнього бізнесу, а також окремих фізичних осіб. Стартапи як недавно створені невеликі компанії з метою продукування інновацій та подальшого їх вигідного продажу для впровадження (вдосконалення) в ширших масштабах найбільш поширені в сфері ІТ-технологій. Основою їх діяльності є здебільшого інноваційна ідея або щойно створена технологія. Перевагою таких форм інноваційної діяльності є

можливості осіб з достатніми трудопотенційними характеристиками, зокрема високими схильностями до інноваційної діяльності, проте дещо обмеженими ресурсними можливостями, вигідно зреалізувати свою інноваційну ідею більш фінансово потужним компаніям. Досить часто стартапи як невеликі компанії дають змогу особам проявити свої трудопотенційні здібності, розвинути їх задля подальшої трудової діяльності (кар'єрного просування) в потужних компаніях з високим рівнем інноваційної активності.

В Україні стартап-бізнес став вимушеною реакцією суспільства з доволі високими інтелектуально-трудовими можливостями на незадовільні умови інноваційної діяльності. Він розвивається використовуючи досвід розвинених країн, зокрема Росії, яка в цьому плані досягла значно кращих успіхів. Динамічність розвитку таких невеликих компаній, що в свій штат часто включають декілька осіб з високими трудопотенційними характеристиками, дали змогу набути певного досвіду в Україні за даним напрямом. Зокрема існують Інтернет-бази даних про стартап-компанії (найбільша з них – UBR [10]). З 2015 року такі українські компанії рейтингуються агентством Pruffi [11]. Перше місце наразі обійняв проект KitApps, який являє собою засіб для створення мобільних додатків для пристроїв, що працюють на платформах Android і iPhone, а також в Інтернеті з використанням підготовлених шаблонів, що сильно спрощує процес створення додатків. Його засновник (у 2012 році) – IT-підприємець віку 26 років [9]. Це яскравий приклад, що такі компанії є відмінною можливістю за умов наявності інноваційної ідеї та професійного підприємницького підходу її практичного втілення в життя з одержанням натомість високих прибутків та перспектив подальшого зростання із залученням у штат інших працівників.

Узагальнення переваг підтримки розвитку стартап-компаній як форми відтворення інтелектуально-трудового потенціалу населення в системі забезпечення інноваційного розвитку економіки України представлено в табл. 3.16.

Таблиця 3.16

Переваги розвитку стартап-компаній як форми відтворення інтелектуально-трудового потенціалу населення України*

№ з/п	Перевага	Сутність	Перспектива
1	Для носіїв інтелектуально-трудового потенціалу		
1.1	Зайнятість у привабливій сфері	Реалізація трудопотенційних характеристик у тій сфері, яка їм відповідає; можливість зайнятості через власну справу навіть за умов високого рівня безробіття.	Створення робочого місця як для самих себе, так і для інших осіб, у т.ч. з розвитком дистанційних форм зайнятості.
1.2	Інноваційна діяльність	Можливість використання інтелектуально-трудового потенціалу.	Набуття важливого в сучасних умовах інформаційного суспільства досвіду.
1.3	Реалізація інноваційної ідеї	Можливість за умов порівняно обмежених ресурсів втілити в життя інноваційну ідею, що матиме значний ефект на ринку.	Доповнення даної ідеї новими інноваційними рішеннями, здатними створити/збільшити попит, сформувати нові потреби суспільства.
1.4	Забезпечення високого рівня доходів	Реальна можливість одержання порівняно високих доходів через реалізацію інноваційної ідеї, причому у молодому віці, аніж при найманій праці чи інших її видах.	Акумуляція фінансових активів задля їх подальшого інвестування, спрямування на реалізацію інших інноваційних ідей тощо.
2	Для бізнесу		
2.1	Посилення конкурентного середовища	Збільшення кількості суб’єктів господарювання малих і середніх форм бізнесу.	Підвищення інноваційної активності суб’єктів господарювання в умовах достатнього конкурентного середовища.
2.2	Пошук інноваційних ідей для подальшого впровадження	Можливість доступу більших фірм до інноваційних ідей стартап-компаній з подальшим їх впровадженням.	Покращення результатів діяльності, якісних характеристик продукції через впровадження інноваційних технологій, вихід на нові ринки.
2.3	Підготовка кваліфікованих кадрів	Можливість залучення у свій штат працівників, що мали досвід діяльності в стартап-компаніях з достатніми трудопотенційними характеристиками.	Посилення конкурентного середовища між персоналом з мотивацією його неперервного розвитку й продуктивної інноваційної діяльності.
3	Для інноваційного розвитку національної економіки		
3.1	Покращення показників інноваційної активності	Вищі (більш якісні) результати інноваційної діяльності через «наближення» генераторів	Розвиток інноваційної економіки зі структурними зрушеннями на користь наукоємних видів економічної

№ з/п	Перевага	Сутність	Перспектива
		інноваційних ідей та тих, хто може їх зреалізувати при наявних ресурсних можливостях.	діяльності.
3.2	Залучення економічно активного населення до продуктивної інноваційної діяльності	Наявність можливостей для осіб, які володіють відповідними трудопотенційними характеристиками, їх реалізовувати.	Попередження демографічних (міграційних) втрат, втрат людського і соціального капіталу.
3.3	Покращення рівня добробуту населення	Можливості одержання достатніх доходів для осіб, зайнятих у стартап-бізнесі, та споживання більш якісної продукції решти населення.	Неперервний розвиток бізнесу з покращенням якості продукції, високим рівнем задоволення потреб суспільства, формуванням його інноваційної культури.

** Розроблено автором*

Ідейна площина діяльності стартапів може диференціюватись значно ширше, аніж у традиційних форм бізнесу. Стартап-проекти можуть бути як суто комерційного характеру, так і охоплювати вирішення соціальних проблем, що також посилюватиме перспективність їх прибутковості. Щоправда тут кінцевим замовником-«великою компанією» повинна бути держава (в особі центральних чи місцевих органів державної влади, органів місцевого самоврядування). Наприклад, за твердженням фахівців, для України прийнятними були б такі ідеї стартапів латиноамериканського походження, що вирізняються і соціальним спрямуванням:

– дешеві освітні курси, які насправді користуються великою популярністю в студентів як спосіб поглиблення знань у сферах, що їх цікавлять;

– програмне забезпечення, що дозволяє швидко одержати лабораторні аналізи при медичному обстеженні;

– сервіс сімейної безпеки з визначенням місцезнаходження членів родини (особливо маленьких дітей);

– Інтернет-платформа з ремонту автомобілів, що дозволяє визначити

об’єктивну вартість відповідних послуг та ін. [1].

Бачимо, що більшість стартап-ідей передбачають онлайн-діяльність. Проте не слід обмежуватись у розумінні стартапів лише віртуальним простором (щоправда найбільш популярними стартапами є проекти електронної комерції й соціальні мережі, що є повністю віртуалізованими компаніями). Для України важливо підтримувати стартап-компанії, що дозволяють використовувати інтелектуально-трудовий потенціал осіб з можливістю інноваційної діяльності в реальних науково-дослідних проектах і з використанням невіртуалізованого матеріально-технічного (непрограмного) забезпечення та продукуванням реального (речового) товару (послуги). Водночас онлайн-стартапи вже одержали позитивний досвід функціонування та не потребують надміру цільової підтримки з боку держави.

Зі стартап-бізнесом тісно пов’язана практика краудфаундингу, яка, разом з тим, має принципові відмінності. Краудфаундинг передбачає реалізацію інноваційних ідей з формуванням ресурсного забезпечення через добровільні пожертвування. Як правило, сутність таких ідей представлена на спеціальних веб-сайтах, доступ до яких має широке коло громадськості, які можуть брати участь у добровільних пожертвуваннях. Таким чином, особа, яка згенерувала інноваційну ідею має змогу розмістити її на сайті (загальна сутність, вартість впровадження) та очікувати реакції читачів щодо перспектив її втілення в життя, що буде виражено в сумі зібраних коштів.

Практика краудфаундингу добре поширена в інноваційно розвинених країнах. Кращим досвідом тут буде США. У даній країні доволі популярним веб-ресурсом є kickstarter.com, де розміщуються інноваційні ідеї. Можливості здійснювати добровільні пожертвування в їх реалізацію мають тільки громадяни США. Так само, щоб представляти свої інноваційні ідеї, треба мати громадянство або діяти спільно з особами, які його мають. В Україні ж наразі діє схожий сайт на принципах «спільнокошту» – biggggidea.com/projects/, на якому подано різні бізнес-ідеї часто соціального, культурно-мистецького характеру, проте серед них фігурують і такі, що мають інноваційний напрям.

Участь у добровільних пожертвуваннях на даному сайті можуть брати не лише громадяни України.

Виходячи з цього, вважаємо, що для активізації інноваційного розвитку економіки України з мотивацією населення до інноваційної діяльності через втілення в життя своїх інноваційних ідей вкрай важливо поширювати сайти за прототипом kickstarter.com. При цьому мають бути спеціалізовані веб-ресурси суто на інноваційних ідеях, які б подавали та брали участь у їх фінансуванні лише громадяни України (або громадяни інших держав, які спільно з ними діють).

У частині відтворення інтелектуально-трудового потенціалу зайнятого населення в системі інноваційного розвитку економіки України (див. табл. 3.15) актуалізується потреба ефективного підвищення кваліфікації з вивченням нових технологій у професії, мов тощо. На даному етапі серед поточних цілей вирішення даного завдання має бути стимулювання самоосвіти населення через різні прогресивні технології. Вважаємо, що наразі актуальним є поширення культури споживання послуг віртуальних освітніх проектів типу курсів «Курсер» на сайті https://www.coursera.org/. Курсер є проектом онлайн-освіти Стенфордського університету. Він може завоювати широку прихильність і серед громадян України, адже дана міжнародна освітня online-платформа вперше запустила навчальний курс «Модельне мислення» (Model Thinking) з українськими субтитрами. Окрім того, планується відкриття у рамках реалізації даного проекту навчального центру в м. Київ. Самоосвіта громадян України через такі проекти насправді є дуже важливою в підвищенні їх інноваційної активності, адже дозволяє краще осягнути переваги використання нових технологій, застосовуваних в онлайн-навчанні, а також значно покращити якість трудопотенційних характеристик населення.

У підсумку слід зазначити, що забезпечення інтелектуально-трудовим потенціалом рушійності інноваційного розвитку економіки України повинно здійснюватись на основі формування загальної інноваційної культури населення. Цього можна досягти системно й послідовно через зусилля,

спрямовані в першу чергу на молодь. Створення можливостей реалізації інноваційних ідей через систему стартапів і краудфандингу, мотивація самоосвіти, розвиток міжпоколінних знаннєвих трансфертів професійного характеру мають стати тим поштовхом активізації інноваційної діяльності, який виведе економіку України на вищий рівень з чіткими ознаками інформаційного суспільства. Водночас необхідним є підвищення інноваційної культури суспільства через розвиток таких загальнодержавних соціальних проектів, як державний реєстр виборця, електронна звітність, електронний уряд (з наданням, для прикладу, послуг онлайн-довідок) тощо. Такі проекти значно змінять світоглядні засади суспільства, забезпечивши відхід від суто індустріальних поглядів з переорієнтацією на нові можливості розвитку й праці.

Список використаних джерел:

1. *Дегтерева А. 8 латиноамериканских стартап-идей, достойных Украины [Електронний ресурс] / А. Дегтерева // Forbes Украина. — Режим доступу : http: //forbes.ua/opinions/1360250-8-latinoamerikanskih-startap-idej-dostojnyh-ukrainy*
2. *Дідківська Л. Державне регулювання економіки : навч. посіб. / Л. Дідківська, Л. Головко. — К. : Знання-Прес, 2000. — 209 с.*
3. *Економічний енциклопедичний словник : у 2-х т. / С. В. Мочерний, Я. С.Ларіна, О. А. Устенко, С. І. Юрій ; за ред. С. В. Мочерного. — Л. : Світ, 2006. – 568 с.*
4. *Про інноваційну діяльність : Закон України від 04.07.2002 № 40-IV, із змінами, в редакції від 05.12.2012, підстава 5460-17 [Електронний ресурс]. — Режим доступу : http://zakon4.rada.gov.ua/laws/show/40-15*
5. *Про наукову і науково-технічну діяльність : Закон України від 13.12.1991 року №1977-XII, із змінами, в редакції від 05.12.2012, підстава 5460-17 [Електронний ресурс]. — Режим доступу: http://zakon4.rada.gov.ua/laws/show/ 1977-12*
6. *Про пріоритетні напрями інноваційної діяльності в Україні : Закон України від 08.09.2011 № 3715-VI, із змінами, в редакції від 05.12.2012, підстава 5460-17 [Електронний ресурс]. — Режим доступу : http://zakon4.rada.gov.ua/laws/show/3715-17*
7. *Програма розвитку інвестиційної та інноваційної діяльності в Україні: Постанова Кабінету міністрів України від 02.02.2011 року №389 [Електронний ресурс]. — Режим доступу : http://zakon4.rada.gov.ua/laws/show /389-2011-%D0%BF*
8. *Прощаликіна А. М. Фінансове забезпечення інноваційної діяльності в Україні [Електронний ресурс] / А. М. Прощаликіна. — Режим доступу : http://archive.nbuv.gov.ua/portal/soc_gum/vchu/N177/N177p048-056.pdf*
9. *Стан корупції в Україні. Порівняльний аналіз загальнонаціональних досліджень: 2007–2009, 2011. Звіт за результатами соціологічних досліджень. — Київ, 2011. — 47 с.*
10. *Стартап проекти України [Електронний ресурс]. — Режим доступу: http://bp.ubr.ua/list/startup-ukraine*
11. *ТОП-30 лучших стартапов Украины [Електронний ресурс]. — Режим доступу : http://ain.ua/2012/10/19/98813*

12. *Чумак О. В. Соціально-філософський аналіз поняття «інновація» та «інноваційна діяльність» / О. В. Чумак // Гуманітарний вісник Запорізької державної інженерної академії: зб. наук. пр. — 2009. — № 36. — С. 152–166.*
13. *Шевчук О. А. Монополія знань як основний чинник економічного зростання в умовах розвитку глобалізації / О. А. Шевчук // Економіка розвитку : науковий журнал Харківського національного економічного університету. — Х. : Вид. ХНЕУ, 2012. — № 2 (62). — С. 81–86.*

3.5. РОЛЬ ВЕРИФІКАЦІЇ В ПРОТИДІЇ ЗЛОЧИНАМ В СОЦІАЛЬНІЙ СФЕРІ ТА ЗАГРОЗАМ СОЦІАЛЬНІЙ БЕЗПЕЦІ

МЕХЕДА НАТАЛІЯ ГРИГОРІВНА*, к.е.н., доцент,*
доцент кафедри економіки підприємства, обліку і аудиту
Черкаського національного університету ім. Богдана Хмельницького

Формування ефективної конкурентоспроможної економіки, поєднання соціального та економічного розвитку суспільства, побудова в Україні економіки європейського зразка неможливі без суттєвого зниження рівня тінізації української економіки. Тінізація економіки спричинює посилення процесів криміналізації економічних відносин, заміну державного контролю кримінальним, поширення корупції в органах державної влади, підриваючи, зрештою, довіру до держави.

Тіньовий сектор економіки має значний вплив на всі соціально-економічні процеси, які відбуваються в суспільстві. Без урахування цього факту неможливе проведення наукового економічного аналізу на макро- і мікрорівнях, ухвалення ефективних управлінських рішень на всіх рівнях. Ігнорування такого багатогранного й суперечливого явища, як тіньова економіка, призводить до значних помилок при визначенні макроекономічних показників, до неадекватної оцінки найважливіших процесів і тенденцій, до тактичних і стратегічних прорахунків під час прийняття відповідних рішень. Час радикальних соціальних, політичних та економічних змін у будь-якій з країн світу характеризується, поряд з іншим, активізацією тіньових проявів в економічній діяльності. НеставвиняткомітрансформаційнийпроцесвУкраїні[7].

Розгортання тіньової діяльності на початку трансформаційної кризи слід розглядати як закономірне явище, пов’язане із руйнуванням старої інституційної системи та командно-адміністративного господарського механізму, у той час як нові важелі економічного регулювання на той час ще не сформовано [2].

Отже, тіньову економіку можна розглядати як об’єктивно обумовлений соціально-економічний механізм, який компенсує упущення та недосконалість

легальних соціально-економічних відносин. Внаслідок цього в країні створюються впливові та чисельні соціальні прошарки, фактично зацікавлені у збереженні економічних деформацій, які сприяють поширенню тіньової економіки [6].

Соціально-економічна природа тіньової економіки в Україні потребуєвирішення проблем соціальної справедливості й соціального захисту, необхідності побудови в Україні суспільства соціальної справедливості та активного впровадження в життя політики і стратегії, спрямованих на її забезпечення, що є шляхом забезпечення соціальної безпеки.

В Декларації про державний суверенітет України соціальна безпека розглядається як "стан гарантованої правової та інституціональної захищеності життєво важливих соціальних інтересів особи й суспільства від внутрішніх і зовнішніх загроз", це стан гарантованості правової та інституційної захищеності життєво важливих соціальних інтересів людини, суспільства і держави від зовнішніх та внутрішніх загроз; стан і характеристика міри досягнення оптимального рівня безпеки функціонування, відтворення і розвитку соціальної системи, яке забезпечується сукупністю здійснюваних державою і суспільством політичних, правових, економічних, ідеологічних, організаційних і соціально-психологічних заходів, які дають змогу зберегти існуючі в суспільстві конституційний устрій, соціальну стабільність, не допускаючи їх послаблення; одна з найважливіших внутрішніх складових національної безпеки, характеристика ступеня соціальної стабільності суспільства; стан суспільства, за якого забезпечується нормальне відтворення суспільства як демографічної популяції, як нації, як народу тощо [5].

Соціальна безпека - це стан життєдіяльності людини та суспільства, що характеризується сформованою, сталою соціальною системою забезпечення соціальних умов діяльності особистості, її соціальної захищеності, стійкості до впливу чинників, які підвищують соціальний ризик. Забезпечення соціальної безпеки в будь-якій країні здійснюється засобами державної, насамперед соціальної політики. Поняття "соціальна безпека" є комплексним, містить

економічні, політичні, соціальні та духовні аспекти, відображає все те, що впливає на середовище існування людини, на якість життя людей, робить суспільство стійким, здатним до розвитку.

Серед науковців відсутня єдина думка та єдиний підхід щодо тлумачення поняття соціальний захист.

Так, наприклад, І. М. Сирота вважає, що термін «соціальний захист» належить до функції держави, яка піклується про матеріальне забезпечення непрацездатних громадян [4]. У свою чергу, В. Ш. Шайхатдінов висловлює думку, щодо соціального захисту входить діяльність держави та органів місцевого самоврядування, громадських організацій, підприємств щодо створення сприятливого навколишнього середовища, охорони материнства та дитинства, здійснення допомоги сім'ї, охорони здоров'я громадян, професійної підготовки громадян, забезпечення зайнятості населення, охорони праці, регулювання заробітної плати та доходів населення, забезпечення громадян житлом, регулювання права власності громадян, матеріального обслуговування та забезпечення непрацездатних та інших осіб, котрі потребують соціальної підтримки. Соціальний захист є практичною діяльністю щодо реалізації основних напрямів соціальної політики. Заслуговує на увагу наукова думка А. Г. Ягодки, яка підкреслює, що соціальний захист є системою законодавчих, економічних, соціальних і соціально-психологічних гарантій, що надає:

а) працездатним – рівні умови для поліпшення свого добробуту за рахунок особистого трудового внеску;

б) непрацездатним і соціально вразливим категоріям населення, насамперед,дітям, молоді, що навчається, інвалідам, пенсіонерам, молодим, неповним та багатодітним сім'ям – переваги в користуванні суспільними фондами споживання, у прямій матеріальній підтримці, зниженні податків

Соціальний захист – це діяльність соціально орієнтованої держави, яка здійснюється через комплекс організаційно-правових та соціально-економічних заходів, метою яких є:

- по-перше, створення для працездатних громадян належних умов для забезпечення своїх соціально-економічних та духовних потреб;

- по-друге, гарантоване забезпечення громадянам, які потребують соціальної допомоги, рівня життя не нижче від прожиткового мінімуму.

В Україні поняття "соціальний захист" почали широко вживати лише на етапі переходу до ринку і як його атрибут, хоча в тій чи іншій формі соціальний захист завжди був притаманний українському суспільству. Формуванню сучасних систем соціального захисту у світі сприяло усвідомлення необхідності створення соціальних амортизаторів ринкових ризиків[4].

Багато людей ще й нині не сприймають термін "соціальний захист" щодо населення загалом, вважаючи, що він стосується лише найнужденніших, або, як часто нині висловлюються, незахищених верств населення. Дедалі частіше соціальний захист передбачає комплекс заходів, спрямованих на створення безпечного соціального середовища людини.

Зокрема, у ст. 46 Конституції України проголошується, що громадяни мають право на соціальний захист, що включає право на забезпечення їх у разі повної, часткової або тимчасової втрати працездатності, втрати годувальника, безробіття з незалежних від них обставин, а також: у старості та інших випадках, передбачених законом[1].

Це право гарантується загальнообов'язковим державним соціальним страхуванням за рахунок страхових внесків громадян, підприємств, установ і організацій, а також: бюджетних та інших джерел соціального забезпечення, створення мережі державних, комунальних, приватних закладів для догляду за непрацездатними.

У найширшому трактуванні соціального захисту до нього включають також заходи з охорони здоров'я, соціальну роботу тощо.Отже,соціальний захист передбачає певний рівень матеріальної забезпеченості, тобто підтримку доходів, захист добробуту.

Результатом цих заходів є стан захищеності або безпека особи, соціальної безпеки не лише окремої особи, а й суспільства загалом. Вона є складовою

національної безпеки, що визначає стан захищеності життєво важливих інтересів особи, суспільства й держави від внутрішніх і зовнішніх загроз, а також від загрози соціальним інтересам.

З поняттям соціальної безпеки як складової національної безпеки узгоджується мета соціального захисту — підтримання стабільності у суспільстві, тобто попередження соціальної напруженості, що виникає у зв'язку з майновою, расовою, культурною, соціальною нерівністю, виявляється у страйках, актах громадянської непокори, сутичках між: окремими групами населення.

Заходи соціального захисту мають подвійну спрямованість. В одних випадках вони покликані надавати пасивну підтримку тим членам суспільства, які з певних причин опинились у скрутному становищі. Пасивна підтримка надається у вигляді соціальної допомоги — допомоги суспільства особі або сім'ї, яка не має достатніх засобів існування. Соціальна допомога по суті є адресною, адже вона надається лише тим, хто її потребує. Через соціальну допомогу соціальний захист виконує лікувальну, реабілітаційну функцію, яка полягає в тому, щоб допомогти людям, які потрапили у скрутну життєву ситуацію, зубожіли, вийти з цього стану і не опинитися на узбіччі суспільства [4].

Водночас ще важливішими є заходи, спрямовані на запобігання ситуаціям, що загрожують добробуту людини, на стимулювання активності особи. Соціальний захист виконує превентивну, запобіжну функцію, захищаючи особу та її сім'ю від втрати доходу, що пов'язано з безробіттям, старінням, хворобою або смертю, і поліпшення добробуту сім'ї через соціальні служби та за рахунок грошової допомоги на виховання дітей. Система соціального захисту включає соціальне страхування, програми зайнятості, охорони здоров'я тощо.

Отже, соціальний захист передбачає як пасивні, так і активні засоби підтримки доходів. Пасивними заходами є соціальна допомога, активними — соціальне страхування (тобто забезпечення доходів на випадок втрати

працездатності чи роботи), лікування і профілактика хвороб, сприяння здобуттю освіти й підвищенню кваліфікації.

Економісти ж виділяють три сфери тіньовоії економіки: неофіційна економіка

– легальні види економічної діяльності, у рамках яких має місце не фіксоване офіційною статистикою виробництво товарів і послуг, приховання цієї діяльності від податків; фіктивна економіка

– хабарництво, приписки, спекулятивні угоди й інші види шахрайства, зв'язані з одержанням і передачею грошей; підпільна економіка

– усі заборонені законом види економічної діяльності. Деякі види діяльності з часом легалізувалися, як, наприклад, до XIX ст. лихварство.

Інші – навпаки, опинилися “поза законом” (гральний бізнес в Україні). А деякі види діяльності завжди лишалися “в тіні”.

Тіньова економіка існує майже в усіх сферах соціально-економічних відносин: від дрібного підприємництва до великих корпорацій або навіть центральні органи влади. Приклади можуть бути абсолютно різними. Основні з них: нелегальна заробітна плата (заробітна плата в конвертах) чи виплата з/п не по трудовому договору, а по цивільно-правовій угоді (уникнення сплати соціальних внесків); готівкові операції, що не обліковуються; приховування доходів та/або перебільшення видатків; заниження ціни акцій корпорації при оформлені продажу контрольного пакету; хабари; “відкати”; відмивання коштів; підпільне виробництво; незаконна діяльність; шахрайство; незаконні ринки збуту (так звані “чорні ринки”).

Тіньова економіка становить реальну загрозу національній безпеці та демократичному розвитку держави, негативно впливає на всі сфери суспільного життя: економіку, політику, управління, соціальну та гуманітарну сфери.

Термін "соціальний захист" вживається лише кілька років. Він замінив термін "соціальне забезпечення", який зберігає право на існування, проте характеризує дещо вужче поняття, ніж соціальний захист. Соціальне забезпечення є складовою системи соціального захисту і виконує функцію

накопичення та розподілу коштів соціального захисту, призначених для соціальної допомоги, виплат по соціальному страхуванню та ін.

Соціальне забезпечення включає пенсії та різні види допомоги (по тимчасовій втраті працездатності, по вагітності й пологах, по догляду за дитиною до 3 років, по догляду за хворою дитиною, на поховання, допомогу непрацездатним особам, дохід яких менший від встановленої межі малозабезпеченості, тощо).

Соціальне забезпечення передбачає також подання допомоги в натуральному вигляді (обслуговування інвалідів, людей похилого віку у спеціалізованих установах — будинках-інтернатах і вдома). За радянських часів всі соціальні виплати здійснювала виключно держава.

Тому під соціальним забезпеченням розуміють переважно державне соціальне забезпечення, тобто яке здійснюють державні органи. Отже, соціальне забезпечення — це заходи матеріальної підтримки особи та сім'ї з боку держави, це програми соціальної допомоги, що відіграють роль сітки соціальної безпеки [4].

Суб'єктами, які забезпечують реалізацію належних особам прав на соціальне забезпечення, є:

а) суб'єкти, що безпосередньо надають таке забезпечення:

- ті, які це роблять відповідно до законодавства (державні органи спеціальної компетенції, соціальні страхові фонди, спеціалізовані державні підприємства та установи)

- ті, які надають його на добровільній основі;

б) суб’єкти, які сприяють особам у його отриманні. Суб’єктами права соціального забезпечення виступають такі державні органи:

- Міністерство праці та соціальної політики України;

- Міністерство України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи;

- обласні і районні управління праці та соціального захисту;

- Фонд України соціального захисту інвалідів;

- органи державної служби зайнятості.

Основною функцією кожного з цих органів є надання населенню в межах своєї компетенції різних видів соціального забезпечення. Головними з повноважень цих суб'єктів є їх обов'язки саме у сфері соціального забезпечення громадян.

Найбільш відомим спеціально уповноваженим суб'єктом у сфері соціального забезпечення є Міністерство праці та соціальної політики України. Міністерство праці та соціальної політики України належить до так званих функціональних міністерств. Це означає, що сфера його діяльності визначається соціальною функцією держави, тобто цей орган має забезпечувати реалізацію та захист соціальних прав громадян.

Основними завданнями Міністерства праці та соціальної політики України є:

1) участь у формуванні та забезпеченні реалізації державної політики у сфері зайнятості, соціального захисту населення, у тому числі ветеранів війни, праці, військової служби та громадян, які постраждали внаслідок Чорнобильської катастрофи, соціального страхування, оплати, нормування та стимулювання праці, умов праці, пенсійного забезпечення, соціального обслуговування населення, соціально-трудових відносин, трудової міграції;

2) керівництво діяльністю державної служби зайнятості, проведення заходів, пов'язаних з ефективним функціонуванням ринку праці, сприяння раціональній, продуктивній і вільно обраній зайнятості, підвищенню якості і конкурентоспроможності робочої сили;

3) розроблення і здійснення заходів для посилення мотивації до праці, вдосконалення її оплати, організації та нормування;

4) забезпечення через систему підпорядкованих йому органів реалізації права громадян на соціальний захист шляхом своєчасного та адресного надання соціальної підтримки, в тому числі державної допомоги малозабезпеченим громадянам, у разі втрати роботи, працездатності, досягнення пенсійного віку тощо;

5) забезпечення розвитку соціально-трудових відносин та захисту прав працюючих громадян шляхом здійснення державного нагляду за додержанням роботодавцями вимог законодавства про працю;

6) розроблення заходів, спрямованих на реалізацію політики грошових доходів населення;

7) забезпечення здійснення Пенсійним фондом України заходів у сфері пенсійного забезпечення та соціального страхування.

На місцевому рівні державними органами, наділеними повноваженнями у сфері соціального забезпечення населення, є головні управління праці та соціального захисту населення обласних державних адміністрацій.

У сфері соціального забезпечення діють також спеціалізовані органи, до повноважень яких віднесено соціальне забезпечення окремих категорій громадян. Такими є Державна служба зайнятості, що має своїм завданням соціальний захист безробітних, Фонд України соціального захисту інвалідів, а також Міністерство України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи.

Одним із суб'єктів права соціального забезпечення, на який законодавством покладено здійснення соціального захисту окремих категорій громадян, є Міністерство України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи. Це Міністерство є розпорядником коштів Фонду для здійснення заходів щодо ліквідацій наслідків Чорнобильської катастрофи та соціального захисту населення, який існує у вигляді окремого рахунку Державного бюджету України і не є самостійним суб'єктом права. Суб'єктами права соціального забезпечення виступають також інші особи, які надають матеріальне забезпечення громадянам завдяки цьому Фонду.

Справами соціального захисту інвалідів займається в Україні Фонд соціального захисту інвалідів. Цей Фонд є урядовим органом державного управління, який діє у складі Міністерства праці та соціальної політики України і підпорядковується йому.

Основними завданнями Фонду є:

- участь у реалізації державної політики у сфері соціального захисту інвалідів;
- здійснення контролю за додержанням підприємствами, установами і організаціями всіх форм власності і господарювання нормативів робочих місць для забезпечення працевлаштування інвалідів.

Важливими суб'єктами права соціального забезпечення можна вважати соціальні страхові фонди. В Основах законодавства України про загальнообов'язкове державне соціальне страхування вони називаються цільовими страховими фондами - це органи, які здійснюють керівництво та управління окремими видами загальнообов'язкового державного соціального страхування, провадять збір та акумуляцію страхових внесків, контролюють використання коштів, забезпечують фінансування виплат за загальнообов'язковим державним соціальним страхуванням та здійснюють інші функції згідно з затвердженими статутами.

На сьогодні функціонують:

- Пенсійний фонд України,
- Фонд соціального страхування від нещасних випадків на виробництві та професійних захворювань України,
- Фонд загальнообов'язкового державного соціального страхування України на випадок безробіття
- Фонд соціального страхування з тимчасової втрати працездатності

Сплату страхових внесків до яких проводиться через єдиний соціальний внесок.

Суб'єктами, які сприяють одержанню соціального забезпечення, вважаються юридичні особи, які здійснюють правовстановлюючу діяльність. До них належать:

- органи медико-соціальної експертизи,
- комісії із встановлення пенсій за особливі заслуги перед Україною,
- органи, які видають посвідчення, що підтверджують відповідний

статус (посвідчення учасника бойових дій, посвідчення ветерана війни, посвідчення інваліда війни, посвідчення біженця, посвідчення учасника ліквідації наслідків аварії на Чорнобильській АЕС і потерпілого внаслідок Чорнобильської катастрофи) тощо.

Ще одним суб'єктом права соціального забезпечення, основним завданням якого є ухвалення правовстановлюючого рішення, є Комісія з встановлення пенсій за особливі заслуги перед Україною при Кабінеті Міністрів України. Комісія ухвалює рішення про призначення громадянинові пенсії за особливі заслуги перед Україною, яке надсилається органу, що провадить виплату пенсії. Отже, як і медико-соціальна експертна комісія, Комісія зі встановлення пенсій за особливі заслуги перед Україною при Кабінеті Міністрів України лише ухвалює рішення про встановлення права на соціальне забезпечення (у вигляді пенсії), а виконання його, тобто надання відповідного виду соціального забезпечення, покладається на інші органи.

Об’єктами соціального забезпечення України є наступні [4].

Пенсії — це регулярні грошові виплати, які отримують громадяни від держави та спеціальних фондів після досягнення встановленого віку, у разі інвалідності, втрати годувальника, за вислугою років. Їхніми характерними ознаками є:

- грошові виплати за віком та у разі непрацездатності, коли особа звільняється від обов’язку працювати або не може працювати за станом здоров’я;
- виплати зі спеціальних фондів;
- розмір залежить в основному від одержуваного заробітку.

Вітчизняне законодавство передбачає виплату двох видів пенсій: страхових та спеціальних.

Страхова пенсія — це щомісячні грошові виплати, які здійснюються застрахованим громадянам при досягненні ними пенсійного віку, встановленні інвалідності чи у зв'язку з втратою годувальника за кошти соціальних страхових фондів у порядку і розмірах, визначених законами України «Про

загальнообов'язкове державне пенсійне страхування» та «Про недержавне пенсійне забезпечення».

Страхова пенсія передбачає три види пенсійних виплат, які призначаються та виплачуються особі окремо у солідарній, накопичувальній обов'язковій та недержавній пенсійних системах. У кожній з них особа має право лише на один, визначений законом чи пенсійним контрактом, вид пенсії.

У солідарній пенсійній системі особа має право на пенсію за віком, по інвалідності та у зв'язку з втратою годувальника. Накопичувальна обов'язкова система передбачає виплату довічної пенсії або одноразової пенсійної виплати, а система недержавного пенсійного забезпечення — довічної пенсії, пенсії на визначений період або ж одноразової пенсійної виплати.

Другим видом пенсійних виплат є Спеціальні пенсії. Умови та порядок призначення таких пенсій встановлюються спеціальним законодавством, яким визначається особливий правовий статус осіб, що виконують державні чи інші суспільно значущі функції, мають особливі заслуги перед державою, а також ті, що постраждали внаслідок техногенних та екологічних катастроф. Тому при визначенні пенсійного забезпечення таких осіб використовується декілька відповідних законодавчих актів.

За суб'єктами, що мають право на спеціальні пенсії, їх поділяють на пенсії для:

— військовослужбовців, осіб начальницького та рядового складу внутрішніх справ;

— осіб, які виконують обов'язки державної служби (державні службовці та прирівняні до них особи, посадові особи місцевого самоврядування, народні депутати, судді та службові особи органів прокуратури);

— наукових (науково-педагогічних) працівників; осіб, які мають особливі заслуги перед країною;

— осіб, які постраждали внаслідок Чорнобильської катастрофи.

Допомоги — це такі грошові виплати (крім пенсій) громадянам у випадках, передбачених законом, що надаються з фондів соціального

страхування та за рахунок державного бюджету.

Види допомоги відрізняються між собою їхньою безпосередньою метою та низкою юридичних ознак.

Допомоги можна класифікувати за періодичністю виплат (одноразові та регулярні), за їхньою метою (у разі тимчасової непрацездатності, у зв'язку з народженням дитини та ін.).

Однією зі складових тіньової економічної діяльності є протизаконна діяльність, у тому числі економічна злочинність, характер якої якісно змінився і розширився під дією процесів глобалізації, зокрема, і на соціальну сферу [8].

Корупція та економічний кримінал провокує хаос та економічну нестабільність у соціальній сфері. Кримінальна економіка бруднить господарські відносини, а корупція розбещує апарат владних структур і знижує ефективність державної політики, і соціальної політики в тому числі. Ці явища загрожують не лише економічній, а й соціальній і національній безпецідержави.

Отже, із західної літератури до нашого внутрішнього вжитку за позичено такі терміни: «тіньова економіка», «неоформальна економіка», «скрита економіка», «неофіційна економіка», «вторинна економіка», «чорна економіка», «таємна економіка», «нелегальна економіка», «друга економіка», «чорний ринок» та інші. Даний перелік термінів відображує не стільки відсутність єдності щодо понятійного розуміння, скільки віддзеркалює різні аспекти і структурні складові «тіньової» економіки, а також підкреслює внутрішню якісну складність цього феноменального явища суспільного життя.

Як органічна складова економіки будь-якого суспільства, тіньова економіка являє собою господарсько-комерційну діяльність в різних сферах функціонування держави, яка внаслідок певних причин, прагне уникнути державного обліку та контролю.

Витрати на соціальну сферу є фактичним гальмом економічного зростання. У 2014 році витрати Пенсійного фонду у відсотках до ВВП склали 15,7%, на соціальний захист – 3,7%, що є найбільшими показниками соціальних витрат в

світі. Непомірно роздуті, необґрунтовані витрати на цю сферу, що роками накопичувалися внаслідок соціального популізму, коли гроші виплачувалися не адресно нужденним, а всім без винятку, не вирішують питання соціальної захисту та фактично є гальмом для економічного зростання країни. Ці проблеми суттєво загострилася внаслідок анексії Криму, переоформлення пенсіонерів, що знаходяться в зоні проведення АТО, значної кількості біженців, збільшення субсидій на оплату комунальних послуг тощо, що за відсутності належного електронного реєстру, міжвідомчої крос-перевірки даних та надійних інструментів контролю призвели до побудови неефективної системи пенсійного та соціального захисту.

Адже якщо торік було виплачено 18 млрд грн житлових субсидій, що становить 3,1% держбюджету, то в 2016 році на ці цілі закладено 35 млрд грн, а це вже 5% бюджету. І кількість домогосподарств, відповідно, може зрости з 5,5 млн до 6,5 млн. Пов’язано це з черговим підвищенням тарифів на «комуналку»: впродовж року на 50% має зрости ціна на електроенергію (з 1 березня та 1 вересня), суттєво подорожчає природній газ для побутових потреб. Відтак владі доведеться збільшити й розмір компенсацій із державного бюджету.

Протягом 2016 року, з урахуванням виплат Пенсійного фонду, з держбюджету запланували виплатити 350 млрд грн за всіма програмами соцдопомоги. В умовах кризи – це велика сума.

Держава роками займалася популізмом, роздаючи соціальні виплати всім без винятку замість того, щоб вирішувати питання соціального захисту пенсіонерів та уразливих груп. Ці проблеми істотно загострилася внаслідок анексії Криму, переоформлення пенсіонерів, що знаходяться в зоні бойових дій, значної кількості біженців, збільшення субсидій на оплату комунальних послуг. Всі ці фактори, при відсутності належного електронного реєстру і надійних інструментів контролю, призвели до побудови неефективної системи пенсійного та соціального захисту, посилення ознак тіньової економіки в сфері соціального забезпечення та зростання загроз соціальної безпеки та безпеки держави.

Ефективне використання бюджетних коштів залишається однією з важливих проблем виконання бюджету як для України, так і більшості країн світу. Реалізація ефективної політики у сфері державних фінансів посідає важливе місце у процесі регулювання економічного розвитку держави. Тільки належне застосування новітніх форм державного фінансового контролю, до яких належить державний фінансовий аудит виконання бюджетних програм, в управлінні фінансовими ресурсами надасть можливість створити необхідні передумови для здійснення в державі ефективної економічної політики.

Державний фінансовий контроль реалізується державною контрольно-ревізійною службою через проведення державного фінансового аудиту, інспектування та перевірки державних закупівель.

Одним з головних завдань державної контрольно-ревізійної служби є здійснення державного фінансового контролю за використанням і збереженням державних фінансових ресурсів, розроблення пропозицій щодо усунення виявлених недоліків і порушень та запобігання їм у подальшому.

Інспектування і аудит ефективності, хоч і близькі за змістом багатьох операцій поняття, проте це різні види контролю.

Державний фінансовий аудит виконання бюджетних програм (аудит ефективності) – це форма контролю, спрямована на визначення ефективності використання бюджетних коштів для запланованих цілей та встановлення факторів, які цьому перешкоджають. Результати аудиту ефективності та їхня оцінка викладаються в аудиторському звіті.

Інспектування полягає у документальній і фактичній перевірці певного комплексу або окремих питань фінансово-господарської діяльності об'єкта контролю і проводиться у формі ревізії, яка має забезпечувати виявлення фактів порушення законодавства, встановлення винних у їхньому допущенні посадових і матеріально відповідальних осіб. Результати ревізії викладаються в акті.

Ефективність соціального інспекторату низька і потребує подальшого удосконалення.За попередніми підрахунками, один соціальний інспектор мав би перевіряти 37,2 тис. виплат на рік або 101 виплату в день.

Виходячи з вищенаведеного, можна стверджувати, що поняття «аудит ефективності» ширше від поняття «інспектування», оскільки охоплює не лише перевірку достовірності фінансових показників, але і здійснення оцінки стану досягнення запланованих показників (продукту, ефективності, якості), виявлення проблем у виконанні бюджетної програми та розробка пропозицій щодо їхнього усунення.

В сучасних умовах розвитку все більше наголошується на необхідності оцінки ефективності та результативності управління державними ресурсами. Мова йде про модернізацію контролю, який би мав спрямованість на проведення глибокого аналізу та оцінки системи державного управління в різних сферах з точки зору ефективності, результативності, а не тільки встановлення законності операцій та цільового використання коштів, як це традиційно прийнято під час інспектування. Тим більше, що без ефективної системи контролю в системі державного управління неможлива побудова високорозвиненої, демократичної держави.

Верифікація – комплекс заходів, спрямованих на підтвердження достовірності наданих даних отримачів соціальних допомог.Завданням при проведення верифікації є не лише виявлення порушень, а й повідомлення розпорядника коштів про виявлення порушення і надання рекомендації. .

Верифікація - підтвердження достовірності даних про пенсіонерів і одержувачів соціальних виплат - є однією з ключових реформ, необхідних для наведення порядку в видаткової частини державного бюджету. Вона дозволить впоратися з шахрайством і розкраданнями в сфері пенсійного та соціального забезпечення - наприклад, вирішити знамениту проблему "мертвих душ" (померлих людей, за яких хтось інший продовжує отримувати належні їм виплати). Законодавство, потрібне для початку цього процесу, було прийнято в рамках "бюджетного пакету".

Процес верифікації не передбачає штрафи, а передбачає лише аналіз даних, отриманих з різних джерел. Якщо виявлять порушення – повідомлять профільне міністерство, яке і прийме рішення про призупинення виплат.

Верифікація це в жодному разі не скасування соцвиплат. Вона не загрожує чесним громадянам. ЇЇ мета – виявити шахраїв і тих, хто явно не має права на отримання такої соціальної допомоги. Верифікація не створить дискомфорту громадянам.

Міністерство фінансів України презентувало план верифікації (перегляду) соціальних виплат і пенсій для з'ясування того, що кошти, які сьогодні виділяються Пенсійним фондом та іншими державними установами (соціальні фонди, Міністерство соціальної політики України) отримують справжні пенсіонери, справжні громадяни, а не «мертві душі» або «шахраї».

Статки кожного отримувача соціальної допомоги чи субсидії в Україні перевірять органи Міністерства фінансів. Проводити першу за всю історію незалежної України верифікацію (підтвердження достовірності щодо майнового стану, у тому числі отримання інформації про рахунки в банках) Мінфіну дозволив парламент наприкінці минулого року, а нещодавно Кабмін ухвалив усі необхідні для цього процесу документи.

У зв'язку з анексією Криму і війною на Донбасі в країні активізувалася внутрішня міграція. В Україні на 1 лютого 2016 року взято на облік понад 1,7 млн переселенців з Донбасу і Криму.

Коли вирішували, як проводити виплати переселенцям, то всі процедури були заточені на те, щоб надавати допомогу в спрощеному порядку, без безлічі документів. Спрощений порядок створює більше можливостей для зловживань.

Проблема з недобросовісними реципієнтами недавно знайшла несподіваний поворот. Уряд зупинив соціальні виплати для 150 тис осіб, які отримували грошову допомогу по документам нібито переселенців.

Зупинили виплати для 150 тис так званих переселенців. З'ясовано, що шахраї отримують документи громадян, які не проживають на контрольованій території України, йдуть в органи соцзахисту і під приводом того, що вони

нібито зареєстровані як тимчасові переселенці, отримують сотні мільйонів гривень з держбюджету .

"Мертві душі" і зловмисники, безумовно, є, але так чи інакше всі ці схеми були у відповідальності Мінсоцполітики. Тобто, верифікацію розглядають не тільки як спосіб очищення соціальних видатків бюджету, але і як спробу втрутитися в тіньові потоки відомства, що забезпечує соціальний захист.

Проблем і перешкод проведенню верифікації багато.

Згідно з документами, Нацбанк, Пенсійний фонд і фонди державного страхування, банки, інші установи та організації будуть надавати Мінфіну дані. Мова про одержувачів субсидій, пільг, зарплат, пенсій та інших видів соцдопомоги, які виплачуються з центрального і місцевого бюджетів.

Для необхідного ефекту потрібно, щоб всі системи адміністрування соціальних виплат і бази даних зіставлялися між собою. В ідеалі для цього потрібна єдина система обліку одержувачів соцвиплат.

Створити систему на базі стандартів обліку доходів громадян намагалися в 2007-2012 роках на кошти Світового банку. Адекватного технічного рішення і програмного продукту не отримали.

Заразіснує понад сто видів соціальних виплат. На центральному рівні адмініструються дві бази даних їх одержувачів - інвалідів і переселенців. Ще понад десяти баз ведуть місцеві органи влади.

Найбільша складність - забезпечити Мінфіну доступ до всіх даних.

Наприклад, щоб система працювала в режимі онлайн. Такий режим спрощує вимоги до програмного забезпечення і дозволяє приступити до верифікації якнайшвидше.

Пряме відношення до верифікації мають два міністерства - соціальної політики і фінансів. Потрібна інформація від Мінсоцполітики, Пенсійного фонду, казначейства і ГФС, МВС, яке має забезпечити паспортними даними та даними про одруження. Збір інформації від місцевої влади Мінфін планує здійснити через казначейство, адже вихід грошей на соціальні витрати відбувається через нього. Проблемне питання - хто буде верифікатором на

практиці. Як може відбуватися виявлення шахрая, припинення виплат і їх стягнення?

Як бути, якщо соціальну допомогу в обхід закону допоміг оформити інспектор одного з управлінь? Наскільки доцільно в цьому випадку віддавати функції по стягненню регіональним органам міністерств? Передати повноваження щодо стягнення правоохоронним органам чи"рішення про припинення виплат прийматимуть органи, які їх виділяли, - Мінсоцполітики, Пенсійного фонду, страхові фонди.

Інформація про банківську таємницю, доступ до якої тепер має і Мінфін, запевняє співрозмовник, розголошенню іншим органам не підлягає.

Ще одна проблнма - в оперативній передачі інформації на центральний рівень. З отриманням даних від інших відомств у Мінфіну і Мінсоцполітики виникають складності. По суті, верифікація залежить від того, наскільки швидко вдасться вирішити всі ці питання.

Україна - далеко не перша країна, яка вдається до верифікації пенсіонерів і одержувачів соціальних виплат. Зі зловживаннями та шахрайством в даній сфері стикалися багато країн, а для деяких з них процес верифікації був одним з ключових елементів розв'язання криз державних фінансів.

Напевно, найвідомішим є випадок Грузії. У 2000 році в цій країні частка пенсійних виплат, розкрадали через шахрайські схеми (в основному пов'язані з "мертвими душами"), оцінювалася в 25% від загального обсягу пенсій. Зіткнувшись з таким гігантським масштабом зловживань, грузинський уряд провело верифікацію і налагодило нормальне функціонування системи контролю пенсійних виплат[9].

Трохи менш відомий випадок Греції, яка здійснила реформи по верифікації та налагодженню контролю соціальних виплат в 2011 році. Результатом реформ стало припинення виплат для 200 тис. Осіб (2% від населення країни), які не мали на них права, були мертві, або зовсім ніколи не існували. Наприклад, верифікація одержувачів допомоги для громадян старше 100 років виявила, що в країні жило не 9000 таких людей, як вважалося раніше, а всього 1700 - інші

давно померли, але їх родичі продовжували отримувати за них виплати. В результаті Греції вдалося заощадити на верифікації порядку 800 млн євро в рік, або близько 0,4% від тодішнього ВВП країни.

Втім, Грецією та Грузією приклади верифікації не обмежуються. У країнах з розвиненою соціальною підтримкою і ефективними бюджетними системами цей процес відбувається постійно і вбудований в саму систему соціального забезпечення. Наприклад, австралійський Centrelink - відділ Міністерства соціальних служб, що відповідає за адміністрування соціальних виплат - постійно здійснює зіставлення даних з іншими відомствами (наприклад, податковою службою), щоб перевірити, чи відповідають одержувачі соціальних виплат критеріям їх отримання.

В цілому в інших країнах процес верифікації, як правило, відбувається за допомогою відомості всієї існуючої в державних органах інформації про одержувачів пенсій і соціальних виплат в єдині бази даних. Це дозволяє автоматизовано здійснити комплексні перевірки і виявити невідповідності між статусом одержувачів соцвиплат і тієї чи іншої інформації про них. Наприклад, якщо людина отримує пенсію в Пенсійному фонді, а в базі даних МВС значиться як мертвий, досить імовірно, що його пенсію хтось привласнює шахрайським шляхом.

В Україні ситуація нагадує скоріше грецьку, ніж грузинську. Відомства, відповідальні за здійснення соціальних виплат - в першу чергу Міністерство соціальної політики і Пенсійного фонду - самостійно перевіряють реципієнтів цих виплат за власними даними, без залучення даних інших держорганів. При цьому далеко не всі бази даних таких реципієнтів централізовані і доступні в повній мірі з центральних офісів в Києві. В таких умовах дуже ймовірні великі обсяги зловживань і шахрайства.

Саме тому реформу по верифікації здійснює Міністерство фінансів, яке не було раніше задіяно в перевірках і за замовчуванням зацікавлене в максимально ефективному і економному витраті бюджетних коштів. Експеримент по верифікації переселенців-одержувачів державної підтримки, проведений

Мінфіном у 2015 році, вже дозволив зберегти для країни близько 1 млрд гривень на рік, які розкрадалися через схеми по створенню на папері фальшивих "переселенців", в реальності померлих, ніколи не існували або втратили коли -то документи, на які оформлялися допомогу.

З огляду на, що на пенсії і соціальні виплати припадає близько половини всіх державних витрат в Україні, або більше 20% від ВВП країни, навіть при помірних масштабах шахрайства втрати від нього в грошовому вираженні можуть тягнути на десятки мільярдів гривень.

При цьому законослухняні громадяни від скорочення таких шахрайських витрат нічого не втратять і тільки виграють - верифікація є безболісною з соціальної точки зору.

У той же час, з огляду на можливі масштаби зловживань, бенефіціари корупції в системі соціального забезпечення напевно будуть намагатися всіляко перешкоджати проведенню реформи. Для майбутнього країни дуже важливо, щоб їм це не вдалося.

Досвід інших країн, таких як Грузія і Греція свідчать про значну кількість виявлених зловживань, усунення яких, дозволило нормалізувати систему соціального захисту населення і спрямувати вивільнені кошти на надання соціальної підтримки тим особам, які реально її потребують. Враховуючи великий обсяг пенсійних та соціальних видатків, масштаби заощаджень внаслідок ліквідації шахрайства та зловживань може становити десятки мільярдів гривень.

Отже, при аналізі міжнародного досвіду з’ясовано, що під час верифікації соціальних допомог у Канаді виявляється 3,5 % хибних призначень, а в Україні - 0,9 %.в деяких країнах після верифікації виявлено до 30% некоректних виплат. Завдяки верифікації, потенційна економія для бюджету в 2016 році може скласти мінімум 5 мільярдів гривень. Ці гроші будуть використані для підвищення соціальних стандартів, запланованого на 2016 рік. Ключове завдання верифікації – допомогти виявити серед одержувачів соцдопомоги

шахраїв і "мертві душі", і тим самим забезпечити ефективне використання коштів платників податків

Соціальна підтримка буде надаватися тільки тим особам, які реально її потребують, для чого міністерство планує перейти на систему адресних виплат соціальної допомоги.Для цього має намір провести аудит і верифікацію соціальних виплат і їх одержувачів для оптимізації системи соціального захисту та соціального забезпечення громадян, запобігання зростання ознак тіньової економіки та забезпечення соціальної безпеки.

Список використаних джерел:

1. *Конституція України. Прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року. — К., 1996.*
2. *Бакуменко В. Д. Формування державно-управлінських рішень: проблеми теорії, методології, практики. — К., 2010.*
3. *Бідак В. Гуманістична складова соціальної політики в умовах економічних трансформацій // Україна: аспекти праці. — 2001. —№ 5.*
4. *Борецька Н. П. Соціальний захист населення на сучасному етапі: стан і проблеми. — Донецьк, 2001.*
5. *Вегера С Європейська соціальна хартія і Україна // Україна: аспекти праці. — 2001. —№7*
6. *.Засанська О.А. Теоретичні основи боротьби з тіньовою економікою // Актуальні проблеми економіки - 2009. -№5, с. 76-84.*
7. *Шпитчук А.М. Економічні наслідки тінізації економічної системи // Економіка. Фінанси. Право – 2009. №1, с. 3-6.*
8. *Прокопик О.І.. Шляхи детінізації економіки України та її особливості // Банківська справа - 2008. №2, с. 56-66.*
9. *Свиріпа Н.В. Теоретичні основи боротьби з тіньовою економікою // Економіка та Держава – 2009. №7, с. 43-57.*
10. *Джерело:http://www.klubok.net/article2533.html*

РОЗДІЛ 4
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ МЕХАНІЗМУ ПРОТИДІЇ ЗЛОЧИНАМ У ЕКОНОМІЧНІЙ СФЕРІ

4.1. ПРАВОВЕ ТА ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КОМЕРЦІЙНОЇ Й БАНКІВСЬКОЇ ТАЄМНИЦІ ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ФІНАНСОВИХ УСТАНОВ

КАРБІВНИЧИЙ ІГОР ВОЛОДИМИРОВИЧ*, к.е.н., доцент,*
доцент кафедри менеджменту та економічної безпеки
Черкаського національного університету ім. Богдана Хмельницького

Інститут банківської таємниці в українському праві з'явився порівняно недавно, а його поява, як, свого часу, і у більшості розвинутих країн світу, була зумовлена, в першу чергу, стрімким розвитком економічних відносин у суспільстві, природними процесами становлення і розвитку банківської системи України, які тривають з початку 90-х років по сьогоднішній день.

Правовий інститут банківської таємниці є обов'язковим атрибутом правової системи будь-якої економічно розвинутої країни. Наявність його є не тільки обов'язковою державною гарантією для забезпечення свободи та недоторканості особистого життя громадян, проголошеної як конституціями більшості демократичних країн світу, так і міжнародними договорами. Забезпечення інформації режимом банківської таємниці в країні є одним із необхідних атрибутів для збереження захисту колективних економічних інтересів осіб, що провадять діяльність у сфері бізнесу через правовий інститут юридичних осіб.

Поняття "банківська таємниця" є одним із центральних понять банківського права, оскільки пронизує усі напрямки банківської діяльності.

Науковці вважають, що банківська таємниця — це комплексний інститут, а сам термін припускає дві інтерпретації. У вузькому розумінні *банківська таємниця — це обов'язок банку зберігати в таємниці операції клієнтів від сторонніх осіб, насамперед конкурентів того чи іншого клієнта банку, операції, рахунки та вклади (депозити) своїх клієнтів і кореспондентів*. У широкому розумінні *це різновид службової таємниці, тобто конфіденційна інформація щодо клієнта, яка стала відома службовцю б*анку.[4]

Положення, присвячені основним засадам банківської таємниці, містяться як у загальному, так і у спеціальному банківському законодавстві.

Згідно зі статтею 1076 Цивільного кодексу України банк гарантує таємницю банківського рахунка, операцій за рахунком і відомостей про клієнта.

Відомості про операції та рахунки можуть бути надані тільки самим клієнтам або їхнім представникам. Іншим особам, у тому числі органам державної влади, їхнім посадовим і службовим особам, такі відомості можуть бути надані виключно у випадках та в порядку, встановлених законом про банки і банківську діяльність.

У разі розголошення банком відомостей, що становлять банківську таємницю, клієнт має право вимагати від банку відшкодування завданих збитків та моральної шкоди.

Основні правові засади банківської таємниці закріплені у главі 10 Закону України “Про банки і банківську діяльність”, відповідно до статті 60: «Інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку, є банківською таємницею.».

Банківською таємницею, зокрема, є:

1) відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;

2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди;

3) фінансово-економічний стан клієнтів;

4) системи охорони банку та клієнтів;

5) інформація про організаційно-правову структуру юридичної особи - клієнта, її керівників, напрями діяльності;

6) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;

7) інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;

8) коди, що використовуються банками для захисту інформації.

Інформація про банки чи клієнтів, що збирається під час проведення банківського нагляду, становить банківську таємницю.

Положення цієї статті не поширюються на узагальнену по банках інформацію, яка підлягає опублікуванню. Перелік інформації, що підлягає обов'язковому опублікуванню, встановлюється Національним банком України та додатково самим банком на його розсуд. [1]

Як справедливо відмічає у своєму дослідженні правових питань банківської таємниці Д.О. Гетманцев, частина 2 статті 60 Закону надає невичерпний перелік відомостей, які відносяться до банківської таємниці, у зв'язку з чим пропонує відносити до неї будь-яку інформацію про клієнта, яка стала відомою банку під час співпраці з клієнтом. [6]

Згідно зі статтею 61 Закону України “Про банки і банківську діяльність” банки зобов'язані забезпечити збереження банківської таємниці шляхом:

1) обмеження кола осіб, що мають доступ до інформації, яка становить банківську таємницю;

2) організації спеціального діловодства з документами, що містять банківську таємницю;

3) застосування технічних засобів для запобігання несанкціонованому доступу до електронних та інших носіїв інформації;

4) застосування застережень щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком і клієнтом.

Службовці банку при вступі на посаду підписують зобов'язання щодо збереження банківської таємниці. Керівники та службовці банків зобов'язані не розголошувати та не використовувати з вигодою для себе чи для третіх осіб конфіденційну інформацію, яка стала відома їм при виконанні своїх службових обов'язків.

Органи державної влади, юридичні та фізичні особи, які при виконанні своїх функцій, визначених законом, або наданні послуг банку безпосередньо чи опосередковано отримали в установленому законом порядку інформацію, що містить банківську таємницю, зобов’язані забезпечити збереження такої інформації, не розголошувати цю інформацію і не використовувати її на свою користь чи на користь третіх осіб. [1]

Необхідно розрізняти поняття “банківська таємниця” та “комерційна таємниця банку”. Науковці визначають комерційну таємницю банку як відомості про діяльність кредитної організації, конкретний перелік яких встановлено керівником банку з метою захисту прав та інтересів кредитної організації та доведено до посадових осіб банку з врахуванням правил про відомості, які не можуть бути віднесені до кола об'єктів комерційної таємниці".

На думку А. Ю. Вікуліна, між поняттями “банківська таємниця” та “комерційна таємниця” існує ряд принципових відмінностей, які полягають:

1) у суб'єктному складі осіб, які встановлюють зміст та обсяг відповідної таємниці (банківська таємниця встановлена законодавцем на рівні федерального закону, комерційну таємницю встановлює керівник комерційної організації на свій розсуд, він має право взагалі не встановлювати у підпорядкованій йому організації режим комерційної таємниці);

2) у суб'єктному складі осіб, які є власниками відомостей, які складають відповідну таємницю (власником банківської таємниці по відношенню до відомостей про самого себе є клієнт; власником комерційної таємниці є засновники комерційної організації, тобто, особи, які здійснюють право власності по відношенню до її майна);

3) у тому, що встановлення та дотримання режиму банківської таємниці, а отже, і її захист, є обов'язком всіх службовців кредитної організації та за невиконання її вони несуть дисциплінарну, матеріальну і кримінальну відповідальність; встановлення ж та дотримання режиму комерційної таємниці є не обов'язком, а правом керівника організації, яким він може і не скористатися. [5]

Розкриття банками інформації щодо юридичних та фізичних осіб, яка містить банківську таємницю регламентується статтею 62 Закону України «Про банки і банківську діяльність». Банки мають право розкрити банківську таємницю в наступних випадках:

1) на письмовий запит або з письмового дозволу відповідної юридичної чи фізичної особи;

2) за рішенням суду;

3) органам прокуратури України, Служби безпеки України, Державному бюро розслідувань, Національної поліції, Національному антикорупційному бюро України, Антимонопольного комітету України - на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи - суб'єкта підприємницької діяльності за конкретний проміжок часу;

4) центральному органу виконавчої влади, що реалізує державну податкову політику на його письмову вимогу щодо наявності банківських рахунків;

5) центральному органу виконавчої влади, що реалізує державну політику у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму, на його запит щодо фінансових операцій, пов'язаних з фінансовими операціями, що стали об'єктом фінансового моніторингу (аналізу) згідно із законодавством щодо запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму, а також учасників зазначених операцій;

6) органам державної виконавчої служби на їх письмову вимогу з питань виконання рішень судів та рішень, що підлягають примусовому виконанню відповідно до Закону України "Про виконавче провадження", стосовно стану рахунків конкретної юридичної особи або фізичної особи, фізичної особи - суб'єкта підприємницької діяльності;

7) Національній комісії з цінних паперів та фондового ринку у випадках самостійного подання банком інформації про банк як емітент та

адміністративних даних відповідно до законів про цінні папери та фондовий ринок;

8) за рішенням суду Національному агентству з питань запобігання корупції стосовно наявності та стану рахунків, операцій за рахунками конкретної юридичної особи або фізичної особи, фізичної особи - суб'єкта підприємницької діяльності відповідно до Закону України "Про запобігання корупції";

9) іншим банкам у випадках, передбачених цим Законом та Законом України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення";

10) центральному органу виконавчої влади, що забезпечує формування державної фінансової політики, на його письмовий запит під час бюджетного процесу з метою проведення верифікації і перевірки достовірності інформації, поданої фізичними особами для нарахування та отримання соціальних виплат, пільг, субсидій, пенсій, заробітних плат, інших виплат, що здійснюються за рахунок коштів державного та місцевих бюджетів, коштів Пенсійного фонду України та інших фондів загальнообов'язкового державного соціального страхування, та своєчасного і в повному обсязі їх здійснення, надається інформація щодо відкритих на їхнє ім'я рахунків (поточних, кредитних, депозитних тощо), операцій та залишків за ними. У разі нарахування та отримання соціальних виплат, пільг, субсидій, призначених на сім'ю або домогосподарство, інформація надається щодо кожного з членів сім'ї або домогосподарства;

11) Національному агентству України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів, на його письмову вимогу у зв'язку із здійсненням ним виявлення та розшуку активів, на які може бути накладено арешт у кримінальному провадженні, - щодо наявності та стану рахунків, операцій за рахунками конкретної юридичної або фізичної особи, фізичної особи - суб'єкта підприємницької діяльності.

Вимога відповідного державного органу на отримання інформації, яка містить банківську таємницю, повинна:

1) бути викладена на бланку державного органу встановленої форми;

2) бути надана за підписом керівника державного органу (чи його заступника), скріпленого гербовою печаткою;

3) містити передбачені цим Законом підстави для отримання цієї інформації;

4) містити посилання на норми закону, відповідно до яких державний орган має право на отримання такої інформації. [1]

Суб'єктами збереження банківської таємниці в банку є особи, підрозділи, служби, органи, відомства, установи, які безпосередньо впливають на забезпечення збереження банківської таємниці в діяльності банку.

Класифікація суб’єктів формування системи забезпечення збереження банківської таємниці в діяльності банку:

1. В залежності від приналежності суб’єкта:

- внутрішні,
- зовнішні.

2. В залежності від участі у процесі формування системи збереження банківської таємниці:

- спеціальні,
- напівспеціальні,
- інший персонал банку.

3. В залежності від участі у діяльності банку

- акціонери,
- менеджери банку,
- консультанти та спеціалізовані компанії ,
- державні та недержавні регулятори.

4. В залежності від впливу на банк:

- прямого,
- непрямого.

5. В залежності від легітимності:

- органи державного регулювання,
- саморегулівні організації,
- поза межами законодавчих вимог.

В залежності від приналежності суб'єкти поділяються на:

- *внутрішні суб'єкти* (акціонери, Загальні збори акціонерів, Правління, Наглядова рада, Ревізійна комісія, служба безпеки);
- *зовнішні суб'єкти* (державні органи, підприємства, організації, установи тощо).

В залежності від участі у процесі формування системи збереження банківської таємниці:

– *спеціальні суб'єкти* (фірми, що спеціалізуються на забезпеченні безпеки суб'єктів господарювання, правоохоронні органи; охорона, МЧС; служба безпеки банку);

– *напівспеціальні суб'єкти* (структурні підрозділи банку, які виконують окремі функції забезпечення збереження банківської таємниці - юридичний відділ, фінансова служба, служба корпоративного секретаря тощо);

– *весь інший персонал* банка, який зобов'язаний зберігати комерційну таємницю.

В залежності від участі у діяльності банку:

– *акціонери* (мають право на розробку та прийняття стратегії захисту банківської таємниці);

– *менеджери банку* (розробляють стратегію захисту банківської таємниці та слідкують за виконанням її в процесі діяльності банку);

– *консультанти та спеціалізовані компанії* (компанії (охоронні, аудиторські, консалтингові) надають послуги під час діяльності банку щодо вирішення проблем та вдосконалення захисту банківської таємниці);

– *державні та недержавні регулятори* (здійснюють контроль за процесом діяльності банку).

В залежності від впливу на банк:

– *суб'єкти прямого впливу* (загальні збори акціонерів; менеджери банку; консультанти, які надають послуги банку; інвестори);

– *суб'єкти непрямого впливу* (органи державного регулювання, конкуренти тощо).

В залежності від легітимності:

– *органи державного регулювання* (Національний банк України, Міністерство доходів і зборів, Антимонопольний комітет України, Служба безпеки України та інші);

– *саморегулівні організації* (Асоціація українських банків, Асоціація банків Львівщини тощо);

– *поза межами законодавчих вимог* (фірми, які працюють нелегально або здійснюють операції щодо відмивання коштів; фірми, які хочуть здійснити поглинання чи захоплення банку).

В 90% банків автоматизовані всі процеси, але не всі вони застосували систему захисту інформації.

Близько 15% кредитних організацій цікавить розробка системи захисту індивідуально, а всі інші погоджуються до спільних розробок таких систем.

По статистиці, солідні кредитні компанії витрачають на системи захисту інформації близько 10% річного бюджету.

При створені системи захисту банка, спеціалісти враховують всі можливі ситуації витоку інформації.

В сучасних економічних умовах виникла нагальна необхідність створення ефективно діючої служби безпеки в банку.

Гарантування безпеки банку та забезпечення збереження інформації, що становить банківську таємницю є одним із основних та пріоритетних завдань, що стоять перед усіма структурними підрозділами і всіма працівниками поруч із завданням збільшення прибутку. Ефективний захист банківської таємниці може бути забезпечений лише у разі об'єднанні зусиль керівництва, працівників та акціонерів банку.

Організаційне забезпечення безпеки банку може покладатися на спеціалізовані фірми, що надають послуги безпеки, на структурні підрозділи банку відповідно до їх спеціалізації, а також на спеціально створені підрозділи служби безпеки банку. Аналіз процедури створення та функціонуванні служби безпеки банку, яка передбачає здійснення правових і організаційних заходів.

Основною метою служби безпеки банка є запобігання: збитку в її діяльності за рахунок розголошення інформації та несанкціонованому доступу до джерел конфіденційної інформації; розкраданню фінансових коштів та матеріально-технічних цінностей; знищенню майна та цінностей; порушенню роботи банку тощо.

Об’єктом діяльності служби безпеки банку є:

- фінансова діяльність;
- кадровий склад банку;
- інформаційне забезпечення;
- силове забезпечення банку;
- політико-правове забезпечення;
- ринкова безпека банку тощо.

До основних завдань служби безпеки банку належать:

- розроблення програми безпеки банку, організація та впровадження її у практику роботи підрозділів і установ;
- розроблення структури підрозділів служби безпеки банку та системи заходів безпеки;
- охорона діяльності банку та захист інформації, що становить банківську таємницю;
- координація діяльності підрозділів банку з питань забезпечення його безпеки та збереження інформації, що становить банківську таємницю;
- організація спеціального діловодства, яке унеможливлює несанкціоноване одержання інформації, що становить банківську таємницю;
- виявлення та локалізацію можливих каналів витоку конфіденційної інформації в процесі діяльності та екстремальних ситуаціях;

- організація режиму безпеки усіх видів діяльності, включаючи ділові зустрічі, переговори, наради тощо;
- забезпечення охорони приміщень та інших видів майна;
- організація особистої безпеки керівництва та провідних менеджерів банку;
- оцінка економічних та маркетингових ситуацій та неправомірних дій конкурентів;
- забезпечення взаємодії служби з правоохоронними органами з питань безпеки діяльності банку та його персоналу.

До основних функцій служби безпеки банку належать:

- організація та забезпечення пропускного та внутрішньооб'єктного режиму в приміщеннях;
- участь у розробці статутних та інших господарських документах з метою відображення в них вимог забезпечення безпеки та захисту банківської таємниці;
- розробка та здійснення заходів щодо забезпечення роботи з документами, що містять банківську таємницю;
- виявлення та перекриття можливих каналів витоку конфіденційної інформації;
- організація та проведення службових розслідувань за фактами порушень безпеки підприємства;
- організація охорони приміщень, в яких зберігається інформація, що становить банківську таємницю;
- оцінка зовнішніх загроз діяльності банку та розробка заходів щодо нейтралізації їх впливу.

Зміст завдань щодо захисту таємної інформації банку, які необхідно вирішити його керівництву та службі безпеки:

1. Правового характеру:

• регулювання доступу до інформаційних ресурсів банку представників державних органів і установ;

- регулювання доступу персоналу до інформаційних ресурсів банку;
- установлення відповідальності за посягання на інформаційні ресурси банку.

2. Організаційного характеру:

- категоріювання інформації банку;
- установлення відповідного режиму роботи банку;
- організація спеціального діловодства в банку;
- підбір персоналу для роботи з інформацією, що має обмежений доступ;
- профілактична та виховна робота з персоналом;
- здійснення заходів захисту інформації під час зустрічей, ділових переговорів, конференцій тощо;
- планування дій банку при стихійних лихах, пожежах, терористичних актах, у тому числі і щодо захисту інформації.

3. Інженерно-технічного характеру:

- спеціальне інженерно-технічне обладнання місць зберігання інформації;
- застосування спеціальних технічних засобів для перекриття різних видів каналів витоку інформації;
- застосування технічних засобів охорони та технічна укріпленість об'єктів.

4. Криптографічного характеру:

- шифрування інформації при переданні її через незахищені засоби зв'язку;
- регламентація доступу до баз даних та електронних документів.

5. Програмно-апаратного характеру:

- застосування спеціальних програмних засобів захисту комп'ютерної інформації;
- застосування антивірусних програм;
- забезпечення безперебійної роботи комп'ютерних систем при аварійних ситуаціях;

• виключення можливості перехоплення електромагнітних випромінювань і наводок;

• створення системи страхового копіювання комп'ютерної інформації. [7]

Організаційна структура служби безпеки банка може бути різною залежно від певних факторів, що впливають на його розвиток. Так, головними з таких факторів можна назвати організаційна структура банку; розмір банку; рівень прибутковості; кількість і якість персоналу; особливості розміщення структурних підрозділів; рівень конкуренції на вітчизняному та міжнародних ринках; рівень корупції тощо.

Структура, чисельність та склад служби економічної безпеки визначаються реальними потребами банками і ступенем конфіденційності інформації, що становить банківську таємницю.

При побудові організаційної структури служби безпеки банку слід дотримуватись наступних принципів:

1. Оптимальності – створення мінімально необхідної кількості зв’язків між органами управління.

2. Оперативності та гнучкості – здатність швидко реагувати на зміни в зовнішньому середовищі або у самій структурі.

3. Надійності – гарантія достовірності передачі інформації і безперервність функціонування системи.

4. Простоти і економічності – полягає у відсутності дублювання робіт та у мінімізації витрат на реалізацію цілей.

5. Спеціалізації – цілеспрямування окремих підрозділів на виконання конкретних функцій управління.

6. Незалежність системи управління від окремих осіб – організаційна структура повинна будуватись не під конкретну особу, а навпаки – працівники за своїми здібностями, професійними навиками повинні підбиратися для виконання цілей організації.

У своїй діяльності служба безпеки банку повинна керуватись:

1. Конституцією України;

2. Законами України :

– «Про основи національної безпеки України»,

– «Про інформацію»,

– «Про господарські товариства»;

– «Про акціонерні товариства» тощо.

3. Внутрішніми положеннями та інструкціями:

З урахуванням зарубіжного та вітчизняного досвіду можна визначити наступну структуру служби безпеки великих банків:

– відділ охорони;

– відділ обробки таємних документів та документів з грифом «Банківська таємниця»;

– відділ інженерно-технічного захисту;

– відділ інформаційно-аналітичної діяльності;

– відділ внутрішньобанківської та інформаційної безпеки банку.

Відділ охорони є найбільш чисельним підрозділом служби безпеки банку, до основних функціональних обов'язків якого входять:

- охорона приміщень і будівель,
- охорона майна,
- охорона працівників та грошових коштів;
- охорона перевезень;
- забезпечення режиму доступу;
- контроль відвідувачів і транспорту;
- розслідування випадків порушення режиму.

Відділ обробки таємних документів та документів з грифом «Банківська таємниця» здійснює забезпечення секретності документі, їх зберігання та недопущення розголосу інформації, що становить банківську таємницю.

Відділ інженерно-технічного захисту здійснюють захист електронно-обчислювальної техніки та каналів зв’язку від несанкціонованих доступів. Основними функціями даного підрозділу є:

- виявлення технічних каналів просочування конфіденційної інформації, що становить банківську таємницю;

- виявлення можливих фактів ведення технічної розвідки проти банку;

- застосування технічних засобів для добування інформації проти конкурентів тощо.

Відділ інформаційно-аналітичної діяльності посідає важливе місце в системі безпеки банку. У створених нею базах даних концентрується важлива інформація, що становить банківську таємницю і потребує особливого захисту від несанкціонованого доступу та злочинних посягань. Основними функціями даного підрозділу є:

– збір інформації від підрозділів служби безпеки та інших підрозділів банку щодо питань гарантування корпоративної безпеки;

– обробка отриманої інформації відповідно до структури бази даних, закладеної до інформаційної системи;

– дослідження інформації, що міститься у базі даних, та надання керівництву банку аналітичних оглядів щодо загроз діяльності тощо.

Відділ внутрішньобанківської та інформаційної безпеки банку є структурним підрозділом, на який покладено завдання єдиного (в рамках господарюючого суб’єкта) інформаційного центру із завданнями оброблення та аналізу інформації, що забезпечує ухвалення вищим керівництвом обґрунтованих рішень із найважливіших для інтересів банку питань.

Забезпечення документального збереження інформації, що становить банківську та комерційну таємницю – це перш за все обмеження доступу до неї. Відповідно до Закону України «Про інформацію» за режимом доступу інформація поділяється на відкриту та з обмеженим доступом, а остання на конференційну та таємну [2]. Відповідно банківська та комерційна таємниця відноситься до таємної інформації.

Спеціальне діловодство в банках є централізованим і забезпечується відповідним підрозділом самостійно або разом з службою безпеки. Це залежить від організаційної структури банку, його масштабів та кількості персоналу, які

залучені до роботу з документами (що містять банківську та комерційну таємницю). Основною особливістю документообороту в спеціальному діловодстві є багатоступеневий облік усіх процедур і операцій, що проводяться з документами.

Порядок створення та організація обліку документів, що містять комерційну та банківську таємницю у банку наведено на рисунках 4.1 та 4.2.

Рис. 4.1. Процес розробки документів, що містять комерційну та банківську таємницю. [7]

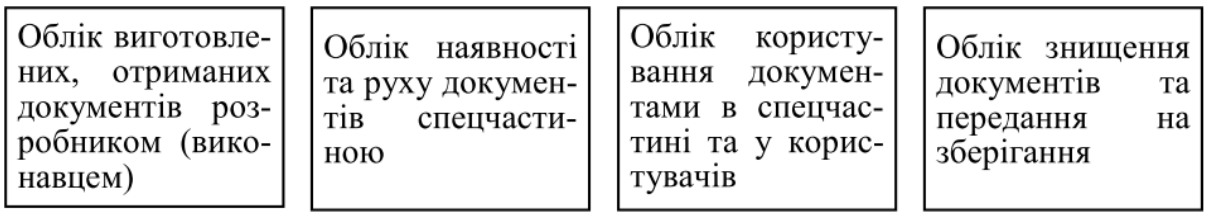


Рис.4.2. Облік документів, що містять комерційну та банківську таємницю. [7]

Оформлення та організація роботи з документами таємного та конфіденційного характеру наведена на рисунку 4.3.

На всіх документах вказується гриф документа: «КТ» Ї комерційна таємниця; «БТ» Ї банківська таємниця; «КІ» Ї конфіденційна інформація	На всіх документах вказується поряд з грифом номер примірника	На звороті останньої сторінки документу вказується кількість примірників, їх місцезнаходження, прізвище виконавця документа та дата його розроблення
Усі документи пересилають тільки в щільних конвертах, на яких вказується гриф документа та його індекс	Документи візуються виконавцем і підписуються посадовою особою, яка має підписувати такі документи	На всіх документах проставляється дата та індекс реєстрації документів за обліком спецчастини

Рис. 4.3. Оформлення документів, що містять комерційну та банківську таємницю. [7]

Захист інтересів банку у взаємовідносинах з персоналом допущених до роботи з банківською та комерційною таємницею, здійснюється через правове закріплення таких взаємовідносин у відповідних документах (рис. 4.4).

Служба безпеки банку для підвищення ефективності захисту таємної інформації повинна створити та керуватися нормативною базою щодо організації роботи по забезпеченню захисту інформації та оперативного реагування на загрози щодо її розголошення. Наведений нижче перелік нормативних документів служби безпеки банку є рекомендованим щодо захисту таємної інформації.

Зобов'язання про нерозголошення інформації банку з обмеженим доступом

↓

Правовий документ, в якому працівник банку добровільно письмово дає згоду на обмеження його прав щодо використання інформації банку з обмеженим доступом.
Одночасно працівник попереджується про відповідальність за розголошення такої інформації

Трудовий договір (контракт)

↓

Наявність у договорі:
- зобов'язань працівника не розголошувати відомості, які становлять таємну або конфіденційну інформацію банку;
- зобов'язань працівника дотримуватися правил захисту інформації з обмеженим доступом, установлених у банку;
- зобов'язань працівника повідомляти безпосереднього керівника і службу безпеки банку про втрату носіїв інформації з обмеженим доступом;
- видів відповідальності працівника за недотримання ним правил захисту інформації

Наказ про призначення на посаду

↓

- визначається ступінь допуску до відомостей, які становлять таємну та конфіденційну інформацію банку;
- визначаються обов'язки працівника та заходи, які повинні ним вживатися для захисту інформації банку

Посадова інструкція

↓

- обов'язок працівника дотримувати у таємниці відомості, які йому стали відомі у зв'язку з його роботою в банку;
- відповідальність працівника за порушення правил зберігання банківської інформації

Рис. 4.4. Правове закріплення факту про нерозголошення комерційної та банківської таємниці. [7]

Основні внутрішні накази та інструкції щодо забезпечення збереження таємної інформації в банку (з зазначенням основного змісту документа):

1. Порядок прийому, переведення та звільнення банку *(1. Підбір, вивчення та погодження кандидатів для роботи в банк, 2. Порядок переведення працівника на іншу посаду, 3. Порядок звільнення працівників, 4. Типові форми)*

2. Інструкція про пропускний та внутрішньобанківський режим банку *(1. Організація та забезпечення пропускного режиму, 2. Види перепусток та порядок їх оформлення, 3. Порядок допуску до приміщень банку, 4. Порядок винесення (вивезення) матеріальних цінностей та майна, 5. Внутрішньобанківський режим, 6. Порядок допуску працівників в приміщення*

банку в неробочий час, вихідні та святкові дні, 7. Обов'язки працівників банку з дотримання та здійснення пропускного та внутрішньобанківського режиму, 8. Порядок видачі і зберігання ключів, 9. Порядок здачі під охорону і зняття з охорони службових приміщень, 10. Дії працівників банку у випадках виявлення порушень відтиску печатки, 11. Відповідальність за невиконання та порушення вимог Інструкції про пропускний та внутрішньобанківський режим банку, 12. Зразки посвідчень, типові форми).

3. Положення про Службу безпеки банку *(1. Задачи службы безопасности, 2. Функции службы безопасности, 3. Полномочия работников службы безопасности, 4. Структура, штатное расписание, кадры службы безопасности).*

4. Наказ Голови Правління банку «Про позачергове інформування про надзвичайні події» (*Надзвичайні події:*

- *Збройний напад на установу банку, терористичний акт, замах на життя працівників філій (відділень), повідомлення про закладку або виявлену вибухівку;*
- *Виявлені у банку крадіжки майна, готівки з кас, інших цінностей;*
- *Стихійні лиха, повені, пожежі, що призвели до руйнування будівель, пошкодження та знищення майна банку та позичальника;*
- *Виникнення, надзвичайних подій, пов'язаних з проведенням інкасації і перевезення грошових та інших цінностей;*
- *Шахрайські дії з використанням платіжних карток, доручень, чеків;*
- *Факти вандалізму з банкоматами та порушення енергозабезпечення та зв'язку банка;*
- *Зняття охорони з банківських установ;*
- *Відвідування з контрольними функціями філії представників НБУ, правоохоронних органів та податкових служб, вказавши конкретно хто прибув, з якою метою, та наявність припису на перевірку;*

- *Надзвичайні пригоди серед персоналу банку (затримання правоохоронними органами, спричинення тілесних ушкоджень, злочинні напади, погрози, нанесення матеріальної шкоди шляхом підпалу майна або його знищення, зникнення без вісті та інше);*
- *Порушення кримінальної справи по заявах банку та проти працівників банку, а також відносно позичальників;*
- *Виникнення дорожньо-транспортних пригод з автотранспортом філії;*
- *Порушення інформаційної безпеки, про вихід з ладу засобів захисту та мережного обладнання, які призвели до тимчасового припинення роботи філії або її підрозділів, або до блокування роботи СЕП з боку НБУ;*
- *Виток конфіденційних відомостей банку;*
- *Факти публікації негативної інформації щодо банку;*
- *Факти недобросовісної конкуренції з боку інших банківських структур регіону;*
- *Виникнення конфліктних ситуацій з органами влади та управління області, гсгіонів;*
- *Надходження претензій та позовів до банку;*
- *Платіжні вимоги, які надійшли до банку від органів Державної виконавчої служби та фіскальних органів для примусового списання коштів з рахунку VIP-клієнтів;*
- *Виявлені банком фальшиві гроші, чеки, сертифікати та інші платіжні засоби;*
- *Несанкціоноване списання коштів з рахунку клієнтів.;*
- *Крадіжки (зникнення) заставного майна;*
- *Зникнення позичальника кредитних коштів;*
- *Раптовий відтік клієнтів та причини, що його викликали.).*

5. Інструкція з організації охорони в установах банка (*1. Вимоги до організації охорони приміщень установ банку, 2. Організація охорони установ банку службою охорони, 3. Обов'язки працівників Служби безпеки з охорони*

установ банку, 3. Організація оборони установ банку, 4. Вимоги щодо обладнання установ банку інженерно-технічними засобами охорони, 5. Умови та порядок приймання установ банку під охорону, 5. Особливості експлуатаційного обслуговування систем ОПС та ТС, 6. Вимоги до технічного стану приміщень установ банку, 7. Організація взаємодії служби безпеки банку з суб'єктами охорони, 8. Організація пропускного режиму в установах банку).

6. Наказ Голови Правління банку «Про заходи щодо захисту відомостей, які складають банківську таємницю та конфіденційну інформацію банку» (Основні додатки до наказу:

•Перелік відомостей, які містять банківську таємницю та іншу конфіденційну інформацію банку;

•Інструкція «Про порядок обліку, зберігання, передачі документів, справ, видань та інших носіїв, які містять відомості, що складають банківську таємницю та іншу конфіденційну інформацію банку» (*1. Облік документів, 2. Використання документів, видань та інших носіїв інформації, зняття грифу «БТ» і «КІБ», 3. Забезпечення збереження документів, видань та інших носіїв інформації. Перевірка їх наявності, 4. Групування документів та інших носіїв у справи*);

•Інструкція «Про порядок надання доступу службовцям до корпоративної мережі банку та прикладних банківських програм. Облік та контроль за наданими правами» ;

•Інструкція "Про порядок надання інформації за межі банку та допуску представників правоохоронних і контролюючих органів для проведення перевірок банку" *(1. Реєстрація, розгляд та надання інформації на запити правоохоронних та контролюючих органів, 2. Допуск представників правоохоронних та контролюючих органів для проведення перевірок);*

•Інструкція "Про порядок виготовлення, видачі, використання штампів та печаток банку" *(1. Порядок виготовлення печаток і штампів, 2. Порядок обліку та видачі печаток і штампів, 3. Порядок вилучення з обігу печаток і штампів, 4. Контроль за обігом та умовами зберігання печаток і штампів);*

•Текст "Зобов'язання працівника банку про нерозголошення відомостей, які містять банківську таємницю та іншу конфіденційну інформацію банку".).

7. Вимоги з технічної укріпленності приміщень відділень банку.

8. Типова Інструкція «Про порядок здавання установ банку під централізовану охорону» (*1. Здача об'єкта під охорону, 2. Зняття об'єкту з під охорони, 3. Порядок використання кнопки тривожної сигналізації, 4. Дії в надзвичайних ситуаціях).*

9. Інструкція «Про порядок прийому та здачі ключів від приміщень банку» (*1. Видача ключів, 2. Прийом ключів*).

10.Інструкція «Про порядок організації охорони індивідуальних сейфів в банку (*1. Вимоги до організації технічної охорони, 2. Обов'язки охорони*).

11.Правила безпеки при здійсненні платіжних операцій та операцій отримання готівки з використанням платіжних карток міжнародних платіжних систем в касах банку.

12.Правила безпечної роботи з клієнтами при емісії платіжних карток та обслуговування в касах банку.

Список використаних джерел:

1. *Закону України «Про банки і банківську діяльність».*
2. *Закону України «Про інформацію».*
3. *Афанасьев Р. Захист банківської таємниці // Прокуратура. Людина. Держава. – 2005. – №2.– С 76-83.*
4. *Ващенко Ю.В. Банківське право: Навч. посібник. – К.: Центр навчальної літератури, 2006. – 344 с.*
5. *Викулин А. Ю. Банковская тайна как объект правового регулирования//Государствово и право. – № 7. – 1998.*
6. *Гетманцев Д.О., Шукліна Н.Г. Банківське право України: – К.: Центр учбової літератури, 2007. – 344 с.*
7. *Зубок М.І., Яременко С.М. Безпека банківської діяльності: підручник. – К. : КНЕУ, 2012 – с. 477.*
8. *Стрельбицька Л.М., Стрельбицький М.П. Основи безпеки банківської системи України та банківської діяльності. – К.: Конор, 2004.– 600 с.*

4.2. ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ

КІБАЛЬНИК ЛЮБОВ ОЛЕКСАНДРІВНА, *д.е.н., доцент,*
завідувач кафедри моделювання економіки і бізнесу
ШУЛЬГА ВІКТОР ІВАНОВИЧ*, к.е.н., доцент,*
НАПОРА ІРИНА ЮРІЇВНА, *аспірант*
кафедри менеджменту та економічної безпеки,
Черкаський національний університет імені Богдана Хмельницького

В умовах посилення інформатизації суспільства, стрімкого розвитку комп'ютеризації банківської діяльності та використання новітніх інформаційний технологій організація інформаційної безпеки банківських установ є одним з актуальних питань.

На сьогодні спостерігається швидкий розвиток інформаційних технологій. Відбувається активний перехід від традиційних банківських операцій до альтернативних шляхів обслуговуванні.

Ефективна робота банківської систем неможлива без забезпечення високого рівня інформаційної безпеки.

Залежно від галузі використання термін «інформація» має чимало визначень. Богуш В. М. визначає дане поняття як «відомості про навколишній світ, процеси, які в ньому відбуваються, про події, ситуації, чиюсь діяльність, що їх сприймають людина і живі організми, керуючі машини та інші системи» [1, с. 243].

Кавун С. В., під «інформацією», розуміє «зафіксоване на носії уявлення про предмети, процеси, події, явища та ін.». Також виділяє такі її властивості, як: конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення; цілісність – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення; доступність – властивість інформації бути захищеною від несанкціонованого блокування [2, с. 7].

Поняття «інформація» визначається і в законодавстві України. Отже, у Законі України «Про захист економічної конкуренції» інформацію розглядають як «відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості» [3].

Згідно Закону України «Про інформацію» ст. 1 інформація – це «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді», а захист інформації, як «сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї» [4].

Не можна не погодитися з думкою Ортинського В. Л. [5], що інформація з погляду безпеки – «це дані, відомості, документи, які мають бути захищеними через їх важливість для суб'єкта діяльності та можливі наслідки від незаконного втручання, розкриття чи розголошування».

Для інформаційної безпеки загрозою є подія, яка впливає на діяльність суб’єкта господарювання та може призвести до її порушення [6].

Під інформаційною безпекою розуміють «стан захищеності інформаційного середовища, захист інформації являє собою діяльність щодо запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, що захищається, тобто процес, спрямований на досягнення цього стану» [7].

Зубок М. І., під терміном «інформаційна безпека банку», розуміє «забезпечення гарантованого захисту інформаційних ресурсів банку від внутрішніх і зовнішніх посягань» [8].

Сліпченко В. І. визначає інформаційну безпеку банку як «організацію гарантованого захисту інформаційних ресурсів банку, відповідну професійна

підготовка працівників у галузі інформаційних технологій, що забезпечує захист інформаційних ресурсів та інформаційних потоків від несанкціонованого доступу до них» [9].

Бодюл Є. М. вважає, що це – «стан захищеності інформації щодо власників, керівництва, клієнтів банку, технологій та інформаційних ресурсів банку від внутрішніх і зовнішніх погроз» [10]. Різник Н. С. розуміє даний термін, як «стан, за якого забезпечується необхідний рівень інформованості керівництва персоналу банку, а також зовнішнього середовища, ефективний захист усіх видів інформації від зовнішніх і внутрішніх ризиків, загроз та небезпек» [11].

Згідно СОУ Н НБУ 65.1 СУІБ 2.0:2010 – розглядається як «збереження конфіденційності, цілісності та доступності інформації; крім того можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність» [12, с. 3].

Дослідивши наукові праці вітчизняних та зарубіжних авторів, пропонуємо авторське трактування терміну «інформаційна безпека банку», під яким розуміємо стан захищеності всіх інформаційних активів банку від внутрішніх і зовнішніх загроз. При цьому під інформаційними активами ми вважаємо будь-яку інформацію, що має цінність для банківської установи, систему її обробки або місце зберігання.

Отже, метою інформаційної безпеки є забезпечення безперебійної роботи з інформацією, забезпечуючи її захист, а при виникненні «збою» звести збитки до мінімуму.

Основними загрозами інформації можуть бути копіювання, знищення, модифікація, порушення доступності (блокування) інформації або нав'язування помилкової інформації [2, с. 34].

Інформаційною безпекою є акумулювання інформаційних ресурсів банківської установи, що відбувається за рахунок системи збору, обробки, зберігання та розподілу інформації із визначенням категорії і статусу, та їх захист через дотримання працівниками, клієнтами та акціонерами правил

роботи з банківською інформацією, своєчасне виявлення каналів витоку інформації [13, с. 46].

Щодо порядку доступу до банківської інформації, то виділяють відкриту інформацію та з обмеженим доступом. Інформація з обмеженим доступом поділяться на конфіденційну та таємну (банківська таємниця, комерційна таємниця) [8, с. 184]. Завдяки класифікації визначаються оптимальні умови захисту тієї чи іншої інформації.

Пріоритетом захисту є банківська таємниця, оскільки банк володіє інформацією щодо фінансової та комерційної діяльності, яка стала відомою у процесі обслуговування, та є довіреною особою своїх клієнтів.

Особливість інформаційної безпеки банківських установ обумовлена тим, що інформація, яка зберігається, має значну фінансову цінність та зачіпає інтереси значної кількості клієнтів і вони розраховують на збереження банківської таємниці; клієнт повинен мати можливість швидко та без перешкод розпоряджатися своїми грошима, оскільки від зручності та спектру запропонованих послуг залежить конкурентоспроможність банку; для роботи з великим обсягом інформації використовують складні високопродуктивні інтегровані системи з використанням специфічного програмного забезпечення та систем управління базами даних [14, с. 236].

Для інформаційної безпеки банку необхідно враховувати специфічні фактори.

По-перше, інформація, яка зберігається в банківській системі є реальними грошима, а їх можна переводити з рахунка на рахунок, здійснювати виплати тощо. Саме через це збільшується кількість злочинів саме в банківській сфері.

По-друге, інформація стосується інтересів клієнтів банку і вони покладаються на захист конфіденційності інформації з боку банку. Отже, банк повинен дбати про інтереси своїх клієнтів, а інакше він ризикує своєю репутацією.

По-третє, від широти спектру запропонованих послуг та зручності співпраці з банком залежить конкурентоспроможність банку.

По-четверте, навіть у позаштатних ситуаціях банк повинен забезпечити високий рівень інформаційної безпеки, оскільки несе відповідальність не лише за свої активи, а й за активи своїх клієнтів.

По-п’яте, важливість інформації, яку зберігає банк про своїх клієнтів, привертає увагу зловмисників [15].

Щодо особливостей інформаційної безпеки банківських установ, для захисту інформації банківської установи основну роль відіграє швидкість і повнота відновлення інформації після збоїв в системі. Банки на такий випадок мають розроблений план щодо відновлення, який періодично вдосконалюється.

Комп’ютеризація діяльності банківських установ підвищила роль інформаційної безпеки в системі економічної безпеки. Для виявлення та усунення внутрішніх та зовнішніх загроз необхідно забезпечити системний підхід в організації системи інформаційної безпеки банківських установ. При розробці засобів захисту слід мати необхідну інформацію про характер можливих загроз.

Незважаючи на численні наукові праці з даного питання на сьогодні немає однозначного трактування терміну «загроза».

Барановський О. І. зазначає, що загроза є специфічною формою ризику. При цьому він вважає, що «…перехід ризику в загрозу починається тоді, коли з'являються негативні якісні зміни в економічних системах, що пов’язані зі значними фінансовими втратами, збитками, які спричиняють банкрутство…» [16, с. 261].

Так, на думку Мігус І. П. поняття «загроза» являє собою певну подію, що впливає на діяльність суб’єктів господарювання, тоді як «ризик» виступає результатом впливу загроз на господарську діяльність суб’єктів господарювання [6].

Як вважає Кавун С. В., загроза – це подія, яка потенційно може порушити одну з властивостей інформації, що захищається [2, с. 32].

Пестовська З. С. трактує загрозу як нереалізовану, але реально існуючу (з певною вірогідністю) можливість нанесення банку будь-якого збитку [17].

Згідно стандарту НБУ загроза це – потенційна причина небажаного інциденту, який може призвести до шкоди для системи або організації [12, с. 4].

На думку Ортинського В. Л., під загрозою безпеці розуміють потенційні дії або події, які можуть прямо чи опосередковано спричинити втрати – призвести до розладу системи, спотворення інформації чи несанкціонованого використання ресурсів мережі, включаючи інформацію, що зберігається, передається або опрацьовується, а також програмні й апаратні засоби [18].

Пропонуємо під поняттям «загроза» розуміти потенційно можливу подію, яка може зашкодити діяльності банківської установи.

Щодо ознак походження загроз, то прийнято розрізняти їх за умисним походженням (викрадання, перехоплення, розголошення, копіювання інформації, несанкціонований доступ тощо) та природним походженням (помилки при обробці інформації, нещасні випадки, стихійні лиха).

Розрізняють об’єктивні та суб’єктивні причини виникнення загроз. Об’єктивними є причини випадкові за характером та непов’язані безпосередньо з діяльністю людини. Суб’єктивні причини пов’язані з діяльністю людини і поділяються на навмисні (наприклад: промислове шпигунство) та ненавмисні (наприклад: недостатня підготовка співробітника) [19].

Шахрайські дії по відношенню до конфіденційної інформації банківської установи можуть здійснювати конкуренти; працівники банку (інсайдери); спецслужби; рейдери; торгівці конфіденційною інформацією; хакери.

Щодо суб’єктів несанкціонованого доступу, то значну частку складає персонал, який добре ознайомлений з технологією обробки інформації. Іноді це можуть бути особи, які відповідають за інформаційну безпеку [20].

Не слід забувати і про клієнтів, що користуються системою дистанційного банківського обслуговування, які нехтують або порушують вимоги щодо безпеки. Не завжди дотримуються клієнти правил користування пластиковими картками. Дану проблему банки намагаються вирішити через роботу з клієнтами та використання технологій.

Основними способами реалізації загроз вважають:

– несанкціонований доступ до інформації,
– протиправний збір інформації (перехоплення, підслуховування),
– маніпулювання інформацією,
– випадкове або навмисне порушенням працездатності технічних засобів прийому, передачі, зберігання і обробки інформації,
– підкуп осіб, які працюють у банку,
– комп’ютерні віруси та шкідливі програми,
– кібератаки,
– стихійні лиха та техногенні катастрофи [21, с. 10].

Питання класифікації загроз інформаційній безпеці знайшло відображення у роботах сучасних дослідників. Так, Страхарчук А. Я., Страхарчук В. П. виокремлюють загрози інформаційній безпеці згідно таких ознак: за цілями реалізації; за принципом впливу на систему; за причинами появи помилок у системі захисту; за об'єктом атаки; за засобами атаки, які використовують [22]. Черевко О. В. класифікує загрози інформаційній безпеці за характером порушення, тяжкістю порушення, передбаченням наслідків, мотивацією, місцем виникнення, закінченістю, об’єктом впливу, причиною виникнення, каналом проникнення, видом реалізації загрози, походженням, розміром збитку [23]. Користін О.Є. виділяє такі групи загроз інформаційній безпеці, як програмні, технічні (у тому числі радіоелектронні), фізичні, інформаційні [24].

Серед способів класифікації найбільш узагальненою, на думку Кавуна С.В., є класифікація за наслідками можливого впливу на інформацію, а саме: загрози порушення конфіденційності, загрози порушення цілісності, загрози порушення доступності [2, с. 33].

Важливим завданням для стабільного та ефективного функціонування основних складових економічної безпеки є виявлення джерел загроз (рис. 4.5). Не можна не погодитися з Яременко С. М., що оптимальним підходом до визначення структури комплексної системи економічної безпеки є ресурсний підхід.

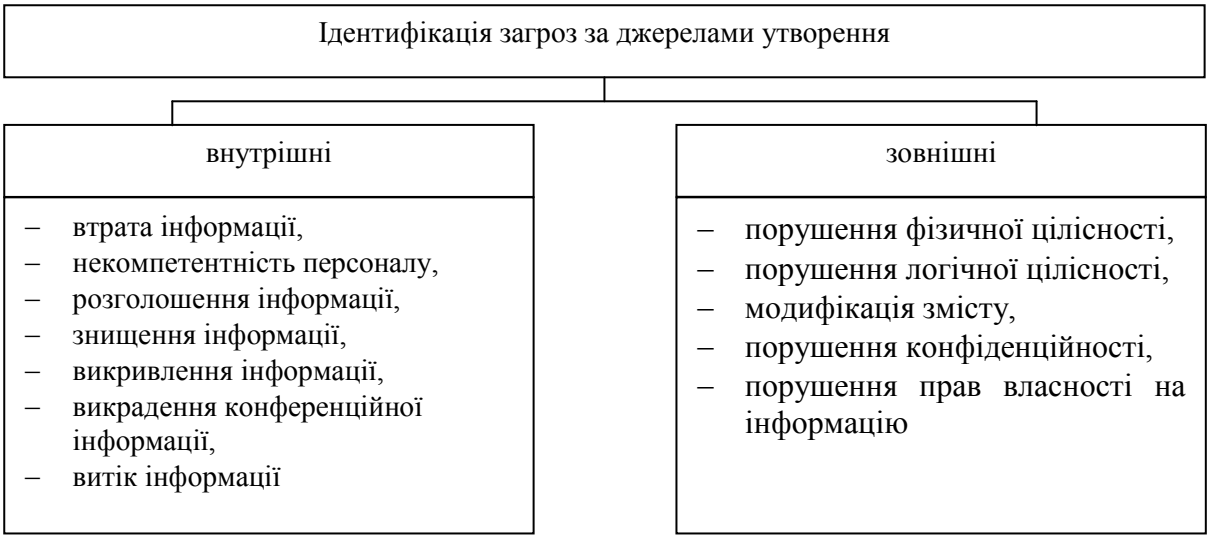


Рис. 4.5. Ідентифікації загроз інформаційної безпеки банківських установ

Розроблено автором на основі: [2, 19, 25, 26].

Оскільки основними ресурсами, які забезпечують діяльність банку є фінансові, матеріальні, інформаційні та кадрові, то структура системи економічної безпеки складається з безпеки матеріальних ресурсів, безпеки фінансових ресурсів, кадрової безпеки та інформаційної. Дії системи економічної безпеки мають бути спрямовані на захисти вищезазначених ресурсів при їх формуванні та використанні [27].

Розглянемо як саме впливає інформаційна безпека банківської установи на інші складові її економічної безпеки (табл. 4.1).

Виокремимо наступні заходи нейтралізації загроз інформаційній безпеці банківської установи:

– технічні (апаратно-програмні) заходи, що перешкоджають впровадженню програм перехоплення ключів та паролів, ненавмисному вчиненню порушення,

– організаційні заходи (регламентація дій, введення заборон, підбір і робота з кадрами, навчання персоналу, посилення відповідальності і контролю, організація зберігання і використання носіїв, сувора регламентація допуску),

– технологічні заходи (застосування спеціальних програм виявлення і знищення вірусів та контроль за помилками операторів введення даних),

– фізичний захист каналів зв'язку,

– резервування критичних ресурсів,

– автоматична реєстрація дій персоналу,

– застосування фізичних і технічних засобів розмежування доступу і перешкоджають несанкціонованої модифікації апаратно-програмної конфігурації АРМ,

– використання додаткових фізичних і технічних засобів захисту тощо [31, с. 23].

Таблиця 4.1

Вплив інформаційної безпеки на інші складові системи економічної безпеки банківської установи

Складові системи економічної безпеки банківської установи	Внутрішні джерела загроз	Зовнішні джерела загроз
Фінансова безпека	– фальшування витрат; – зловживання реальними активами банку чи клієнта; – перевищення повноважень управлінським персоналом; – підробка документів або внесення до них недостовірних даних; – втрата інформації щодо фінансової діяльності банківської установи	– втрата фінансової стійкості банківської установи; – шахрайства з рахунками клієнтів банку; – підроблених платіжних документів і пластикових карток; – крадіжки фінансових коштів
Кадрова безпека	– втрата інформації щодо персональних даних співробітників та керівного складу; – заподіяння майнової шкоди шляхом обману або зловживання довірою персоналу банківської установи; – загроза фізичній і професійній безпеці співробітників та керівного складу	– порушення прав власності на інформацію; – загроза персоналу банку, реалізація якої здатна погіршити стан кадрового напрямку діяльності; – втрата цінного фахівця; – шантаж співробітників та керівного складу
Майнова безпека	– провокування до здійснення або безпосереднього здійснення свідомо збиткових фінансових операцій; – загрози з боку конкурентів, які прагнуть до посилення власних позицій	– погіршення конкурентних позицій банківської установи; – погіршення іміджу банківської установи; – погіршення відносин з клієнтами банківської установи; – дискредитації суперника в очах партнерів і держави

Розроблено автором на основі: [27, 28, 29, 30]

Виявлення та ідентифікація загроз є найбільш важливою задачею для забезпечення інформаційної безпеки банківської установи та економічної безпеки банку в цілому.

Оскільки спостерігається перевага внутрішніх загроз інформаційній безпеці банківських установ над зовнішніми, аналіз вищезазначених середовищ має проводитися комплексно та одночасно.

Управлінню доступу користувачів інформації в мережі приділяється особлива увага. Для даної мети широко використовуються різні програмні системи управління доступом, які навіть можуть заміняти антивірусні програмні засоби. До особливостей також можна віднести використання стандартного, але адаптованого програмного забезпечення для управління доступом до мережі.

Значна увага приділяється організаційно-технічному захисту інформації. В банках рідко використовують шифрування локальної інформації, це пов'язано з високими вимогами щодо швидкодії системи та оперативністю при відновленні інформації.

Співвідношення випадкових і навмисних витоків у банківських установах серйозно відрізняється від загальної картини. Якщо в останньому випадку різниця між показниками навмисного та випадкового витоку інформації незначна, то в банку – частка навмисного витоку інформації становить 68%, у той час, як частка випадкових складає всього 20%. Незначна частка випадкового витоку інформації є наслідком ефективності інформаційної безпеки в банківський сфері. В загальному витоку інформації найбільша частка припадає на персональні данні (близько 88%), а в банках – на фінансову інформацію (до 60 %) [32].

Проведення ідентифікації загроз у сфері інформаційної безпеки банківських установ необхідне для побудови дієвої системи інформаційної безпеки.

При створенні системи економічної безпеки банківської установи інформаційна безпека повинна розглядатися як невід’ємна та вкрай важлива її частина.

Інформаційна безпека банку досягається проведенням збору та аналізом інформації про внутрішнє і зовнішнє середовище банку, аналітичною обробкою інформації щодо партнерів та конкурентів, визначенням категорій банківської інформації та заходів щодо її захисту, дотриманням персоналом банку правил роботи з інформацією, своєчасним виявленням спроб і каналів витоку інформації [33, с. 19].

Необхідний комплексний підхід до організації системи інформаційної безпеки банківських установ.

На нашу думку, систему інформаційної безпеки слід визначати як сукупність суб’єктів, принципів, нормативно-правової бази, політики інформаційної безпеки тощо, з метою виявлення вразливих місць і загроз та запобігання їх впливу на забезпечення нормального функціонування банку.

Визначимо загальну концепцію організації системи інформаційної безпеки банківських установ (рис. 4.6.)

Метою даної системи є забезпечення стійкого функціонування банку, виявлення та запобігання внутрішнім і зовнішнім загрозам інформаційної безпеки банківських установ.

Основними задачами системи інформаційної безпеки є:

– класифікація інформації щодо характеру доступу до неї;

– прогнозування, своєчасне виявлення реальних і потенційних загроз інформаційній безпеці банківської установи та їх усунення;

– створення механізму й умов оперативного реагування на загрози інформаційній безпеці банку;

– пошук способів запобігання або мінімізації збитків, пов'язаних з ймовірними загрозами інформаційній безпеці;

– використання заходів, необхідних для забезпечення інформаційної безпеки банківських установ;

– ретельний відбір кадрів, навчання та підвищення кваліфікації персоналу у зв'язку з особливостями функціонування банківських установ тощо.

– ефективне припинення посягань на інформаційні ресурси банку на основі правових, організаційних і інженерно-технічних заходів і засобів забезпечення безпеки.

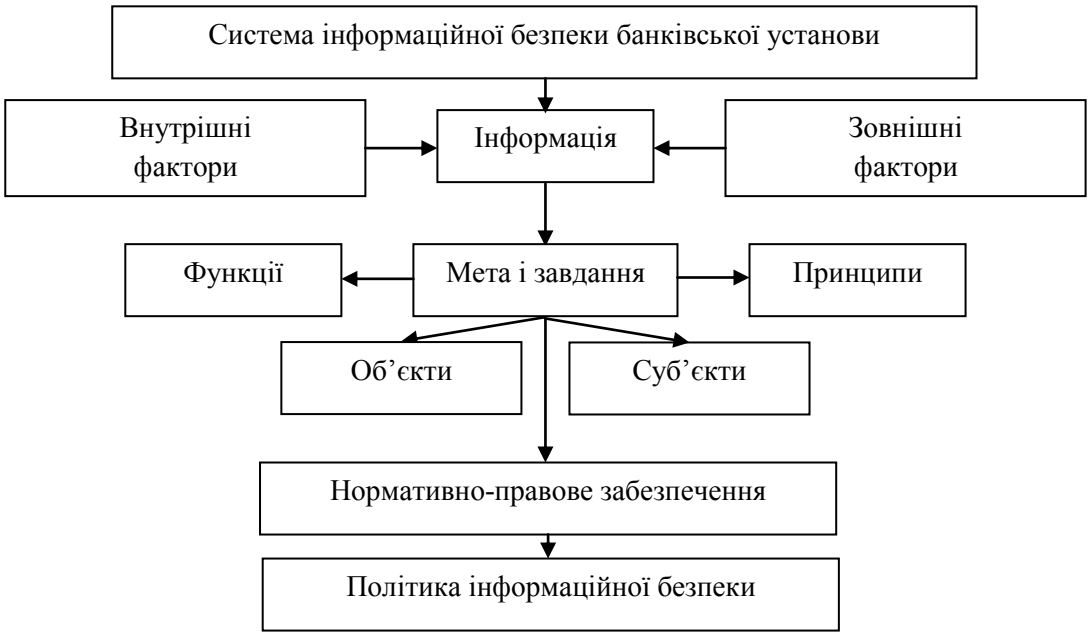


Рис. 4.6. Концепція системи інформаційної безпеки банківських установ.

Організація інформаційної безпеки банків покликана виконувати такі функції:

– захист конфіденційної інформації від неправомірних дій, несанкціонованого доступу, копіювання та знищення;

– організація, координація та корегування виконуваної роботи, пов’язаної з організацією інформаційної безпеки;

– аналіз можливих загроз, ризиків інформаційній безпеці банків;

– аудит інформаційної безпеки банку;

– ліквідація наслідків впливу зовнішніх та внутрішніх загроз.

– проведення із співробітниками банківської установи заходів щодо забезпечення належного рівня інформаційної безпеки та підвищення їх кваліфікації тощо.

На думку С. І. Мельник, складовими елементами системи є об’єкт, суб’єкт і механізм безпеки, а також стратегічні дії із забезпечення безпеки [34, с. 151].

Дудченко Н. В. в своєму дисертаційному дослідженні зазначає, що система, характеризується такими елементами, як: об'єкти, суб'єкти, функції, принципи, механізм забезпечення та методика оцінювання стану системи [35, с. 153].

У редакції Мігус І. П., серед елементів виокремлено: концепцію формування системи, стратегію системи, нормативно-правове регулювання, загрози безпеці, механізм реалізації, методологія оцінки та контролю рівня безпеки [36, с. 312].

На нашу думку, в системі інформаційної безпеки банківських установ поряд з такими елементами, як: об’єкт, суб’єкт, принципи, нормативно-правове забезпечення, слід розглядати політику інформаційної безпеки банку.

Визначимо об’єкти, які підлягають захисту з метою забезпечення інформаційної безпеки банку:

–інформаційні ресурси;

–інформація про персонал;

–програмне забезпечення;

–процеси обробки інформації;

–обладнання автоматизованої системи;

–приміщення.

Серед суб'єктів інформаційної безпеки можна виокремити: державні органи, державні інститути, НБУ, керівники банків, окремі структурні підрозділи банку, юридичні та фізичні особи, які виконують практичні дії із забезпечення інформаційної безпеки банків або вступають з банком у договірні відносини.

Анікін І. В. виділяє наступні основні принципи забезпечення інформаційної безпеки [37]: системності, комплексності, безперервності захисту, розумної достатності, гнучкості управління і застосування,

відкритості алгоритмів і механізмів захисту, простоти застосування захисних заходів і засобів.

Бодюл Є.М. виокремлює такі принципи організації системи інформаційної безпеки банку, як: комплексність, своєчасність, безперервність, активність, законність, обґрунтованість, спеціалізація, взаємодія, удосконалювання, централізація управління, економічна доцільність тощо [38, с. 55].

Вітчизняні та зарубіжні науковці зазначають значну кількість принципів, але автором, враховуючи специфіку діяльності банківських установ, виокремлено наступні:

– принцип законності – забезпечення інформаційної безпеки банківських установ повинно здійснюватися на основі чинного законодавства та в рамках чинних правових актів;

– принцип плановості – вносить організованість у функціонування системи, дозволяє кожному працівнику діяти послідовно, виконувати поставлені задачі та покладені обов'язки;

– принцип компетентності – забезпеченням інформаційної безпеки в банківській установі повинні займатися професіонали, які володіють достатніми знаннями для оцінки ситуації та прийняття правильного рішення;

– принцип превентивності – захист інформації будується таким чином, щоб вживати заходи щодо запобігання виникнення ризиків та загроз. Наслідки реалізації загроз інформаційній безпеці можуть потребувати значно більших матеріальних витрат порівняно з витратами на створення комплексної системи захисту;

– принцип гласності – основні заходи щодо забезпечення інформаційної безпеки повинні бути доведені всім працівникам та беззаперечно виконуватися;

– принцип конфіденційності – способи, заходи та методи забезпечення інформаційної безпеки мають бути відомі лише певному колу фахівців;

– принцип комплексності – для захисту інформації в банківській установі необхідно передбачити комплекс заходів та механізмів захисту (фізичні,

організаційні, програмно-технічні) для вчасного оцінення ситуації та прийняття рішення;

– принцип безперервності – система захисту повинна діяти безперервно та постійно удосконалюватися;

– принцип прозорості – заходи щодо інформаційної безпеки повинні бути непомітними, не заважати користувачам виконувати свої функції;

– принцип адаптивності – система інформаційного захисту повинна будуватися з урахуванням можливої зміни цінності інформації, ступеня конфіденційності, кількості користувачів тощо;

– принцип взаємодії – для забезпечення інформаційної банківської установи банку необхідні скоординовані дії працівників, підрозділів, служб. Всі суб'єкти повинні взаємодіяти один з одним і чітко виконувати свої посадові обов’язки;

– принцип адекватності – рішення повинні прийматися диференційовано, в залежності від ймовірності виникнення загроз, прогнозованого збитку, ступеня конфіденційності інформації та її вартості [39].

Нормативно-правове забезпечення інформаційної безпеки банківських установ визначається законодавчими актами держави. Вони регламентують правила використання, опрацювання та передачі інформації обмеженого доступу та встановлюють ступінь відповідальності за порушення цих правил.

НБУ послідовно впроваджує міжнародну політику в сфері забезпечення інформаційної безпеки банків. Національним банком України з метою підвищення рівня інформаційної безпеки в банківській системі України запроваджено Стандарти з управління інформаційною безпекою в банківській системі України СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги» (ISO/IES 27001:2005, MOD); СОУ Н НБУ 65.1. СУІБ 2.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» (ISO/IES 27002:2005, MOD) тощо [13, с. 46].

Забезпечення інформаційної безпеки банку неможливе без дотримання внутрішніх правил, положень, інструкції тощо.

Доцільно в системі інформаційної безпеки банківських установ також розглядати і політику інформаційної безпеки банку, яка являє собою науково обґрунтовану систему поглядів на визначення основних напрямків, умов і порядку практичного вирішення задач інформаційного захисту банківської установи від протиправних дій.

Політика формується на основі характеристики об'єкта застосування; аналізу поточного стану захищеності інформаційної інфраструктури банку; обліку можливих негативних факторів впливу та ймовірності їх реалізації; створення методології ухвалення управлінських рішень щодо забезпечення інформаційної безпеки з врахуванням вимог, що містяться в законах і нормативних актах, стандартах у галузі інформаційної безпеки [38, с. 53].

За наявності пластикових карт, електронних платежів та глобальної інформаційної мережі, злочинцю не потрібно проникати в банк, йому потрібен лише комп'ютер та мережа «Internet» і можна грабувати будь-які банки та їх клієнтів в усіх частинах світу.

Забезпечення інформаційної безпеки повинне мати безперервний і попереджувальний характер.

На жаль, керівники банківських установ вважають витрати на забезпечення інформаційної безпеки завеликими і не приділяють їй належної уваги. Навіть при виникненні «ситуації», вони воліють її приховати задля збереження власної репутації.

Динамічного розвитку набирає комп'ютеризація та автоматизація банківської діяльності, а отже значення інформаційної безпеки банків буде постійно зростати.

Отже, забезпечення інформаційної безпеки можливе лише при комплексному підході, використанні всіх засобів захисту і на всіх етапах роботи з інформацією. Найкращий ефект досягається тоді, коли всі засоби і методи об'єднуються в єдиний цілісний механізм. При цьому, залежно від

зміни внутрішніх і зовнішніх умов, система захисту повинна оновлюється і удосконалюється.

Список використаних джерел:

1. *Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В. Г. – Київ ООО «Д.В.К.». 2004. – 508 с.*
2. *Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 352 с.*
3. *Закон України «Про захист економічної конкуренції» від 11.01.2001 № 2210-III (редакція від 04.07.2013) [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2210-14.*
4. *Закон України «Про інформацію» від 02.10.1992 р. № 2657-XII зі змінами і доповненнями [Електронний ресурс] – Режим доступу до ресурсу: http://zakon4.rada.gov.ua/laws/show/2657-12.*
5. *Економічна безпека підприємств, організацій та установ: навч. посібник / В. Л. Ортинський, І. С. Керницький, З. Б. Живко [та ін.]. − К. : Правова єдність, 2009. − 544 с. // [Електронний ресурс] – Режим доступу: http://westudents.com.ua/glavy/16613-62-sut-ponyattya-nformats-nformatsyno-bezpeki-zahistu-nformats.html.*
6. *Мігус П. І. Необхідність розмежування понять «загроза» та «ризик» при діагностиці економічної безпеки суб'єктів господарювання [Електронний ресурс] / П. І Мігус., С. М Лаптєв // Ефективна економіка. – 2011. – № 12. – Режим доступу: http://www.economy.nayka.com.ua/index.php?operation=1&iid=821.*
7. *Черевко О. В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту [Електронний ресурс] / О. В. Черевко // Ефективна економіка. – 2014. – № 5. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=3304.*
8. *Зубок М. І. Безпека банківської діяльності: підручник / М. І. Зубок, С. М. Яременко. – Київ: КНЕУ, 2012 – 477 [3]с.*
9. *Сліпченко В.І. Захист банківської таємниці як складова політики безпеки банку// [Електронний ресурс]. – Режим доступу: http://lib.uabs.edu.ua/library/Zbirnik/1042_2010.pdf.*
10. *Бодюл Є.М. Інформаційна безпека банку// [Електронний ресурс] – Режим доступу: http://lib.uabs.edu.ua/library/Zbirnik/1042_2010.pdf.*
11. *Різник Н. С. Безпека банківської діяльності [Електронний ресурс] – Режим доступу: http://lib.lntu.info/books/fof /bs/2011/11-15/.*
12. *СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою» (ISO/ IES 27002:2005, MOD).*
13. *Чернадчук Т. Забезпечення інформаційної безпеки як один із напрямів банківської діяльності / Т. Чернадчук // Юридична Україна. – 2013. – №3. – С. 44-47.*
14. *Жарій Я. В. Актуальні проблеми фінансово-інформаційної безпеки банківської системи України / Я. В. Жарій, Л. В. Дохтаренко. // Вісник Чернігівського державного технологічного університету. – 2013. – №1 (64). – С. 232-239.*
15. *Кириченко О. А. Казначейство банку: Навч. посіб. / О. А. Кириченко, М.П. Денисенко, А. П. Гречан та ін. – К: Центр учбової літератури, 2010. – 464 с. [Електронний ресурс] / Режим доступу: http://b-ko.com/book_179.html.*
16. *Барановський О. І. Фінансові кризи: передумови, наслідки і шляхи запобігання: монографія / О. І. Барановський. – К.: Київ. нац. торг.-екон. ун-т, 2009. – 754 с.*
17. *Пестовська З. С. Індикатори фінансової безпеки банківської діяльності: макро- та мікроекономічний рівень [Електронний ресурс] / З. С. Пестовська //Теоретико-методологічні засади прискорення процесів соціально-економічного розвитку регіону: колект. моногр. / [Ткаченко В. А. та ін. ; за заг. ред. П. І. Сокуренка]; Дніпропетр. ун-т ім. Альфреда Нобеля, Кременчуц. ін-т. - Кременчук : Щербатих О. В. [вид.], 2013. – Розділ 4.7. –*

С. 338-347. – Режим доступу: http://duep.edu/uk/naukovi-publikatsiji-v-ukrajini-i-za-kordonom/kafedra-mizhnarodnih-finansiv-obliku-ta-opodatkuvannja.
18. Економічна безпека підприємств, організацій та установ: навч. посібник / В. Л. Ортинський, І. С. Керницький, З. Б. Живко [та ін.]. −К. : Правова єдність, 2009. − 544 с. // [Електронний ресурс] – Режим доступу: http://westudents.com.ua/glavy/16613-62-sut-ponyattya-nformats-nformatsyno-bezpeki-zahistu-nformats.html.
19. Ревенков П. В. Защита информации в банке: основные угрозы и борьба с ними [Електронний ресурс] / П. В. Ревенков – Режим доступу: http://www.uipdp.com/articles/2011-05/22.html.
20. Гуцалюк М. Безпека банківських інформаційних систем // Центр исследования проблем компьютерной преступности // [Електронний ресурс] – Режим доступу: http://www.crime-research.ru/library/bezp_ba.htm
21. Диба М. Інформаційні ризики в банківській діяльності / М. Диба, М. Зубок, С. Яременко // Вісник Національного банку України. – 2007. – № 9. – С. 28-36.
22. Страхарчук А. Я. Інформаційні системи і технології в банках: навч. посіб. [Електронний ресурс] / А. Я. Страхарчук, В. П. Страхарчук ; НБУ, Ун-т банк. справи. – К. : УБС НБУ – Знання, 2010. – 515 с.– Режим доступу: http://libfree.com/102585050-bankivska_spravainformatsiyni_sistemi_i_tehnologiyi_v_bankah__straharchuk_aya.html
23. Черевко О. В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту [Електронний ресурс] / О. В. Черевко // Ефективна економіка. – 2014. – № 5. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=3304.].
24. Економічна безпека: навч. посіб. [Електронний ресурс] / О. Є. Користін, О. І. Барановський, Л. В. Герасименко та ін.; за ред. О. М. Джужі. – К.: Алерта; КНТ; Центр учбової літератури, 2010. – 368 с.– Режим доступу: http://westudents.com.ua/knigi/113-ekonomchna-bezpeka-koristn-o.html.
25. Кравченко А. М. Особливості захисту інформаційних систем у банківських установах / А. М. Кравченко, А. А. Орєхов, А.Г. Гаркунов // Сучасний захист інформації. – 2013. – №2. – С. 53-55.
26. Ярочкин В. И. Основы безопасности бизнеса и предпринимательства [Електронний ресурс] / В. И. Ярочкин, Я. В. Бузанова. – М.: Академический Проект: Фонд «Мир», 2005. – 208 с. – Режим доступу: http://finances.social/biznesa-osnovyi/osnovyi-bezopasnosti-biznesa.html.
27. Яременко С. М. Комплексна система економічної безпеки банку та її структура / С. М. Яременко // Вісник КЕФ КНЕУ імені В. Гетьмана. – 2011. – №1. – С.213-221.
28. Гончарова К. Г. Кадрова безпека, як складова економічної безпеки банківської установи [Електронний ресурс] / К. Г. Гончарова // Ефективна економіка. – 2015. – № 11. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=4602.
29. Кадрова безпека суб'єктів господарської діяльності: менеджмент інсайдерами / колективна монографія за заг. ред. проф. Мігус І.П. [Текст]. – Черкаси: вид-во «МАКЛАУТ», 2012. – 315 с.
30. Юрін Я. Фінансова і інвестиційна безпека банків та її вплив на загальноекономічну безпеку держави / Я. Юрін, А Сундук. // Вісник Національного банку України. – 2004. – № 7. – С.18-20.
31. Олійник А. В. Інформаційні системи і технології у фінансових установах [Текст]: навч. посібник / А. В. Олійник, В. М. Шацька. - Л.: Новий Світ-2000, 2006. – 436 с. / Режим доступу: http://buklib.net/books/28625.
32. Аналітичні дані [Електронний ресурс]. – Режим доступу: http:// www.infowatch.ru.
33. Зубок М. І. Безпека банківської діяльності: підручник / М. І. Зубок, С. М. Яременко. – Київ: КНЕУ, 2012 – 477 [3]с.
34. Мельник С. І. Формування системи економічної безпеки банку / С. І. Мельник // Вісник економіки транспорту і промисловості. – 2010. – № 29. – С. 149-152.

35. *Дудченко Н. В. Вплив державного регулювання на систему економічної безпеки банківських установ: дис. канд. ек. наук: 21.04.02 / Н. В. Дудченко – Черкаси, 2013. – 270 с.*
36. *Мігус І. П (Шульга І. П) Економічна безпека емісійної діяльності акціонерних товариств: [монографія] / І. П. Мігус (І. П. Шульга). – Черкаси: ТОВ «МАКЛАУТ», 2010. – 425 с.*
37. *Аникин И. В. Теория информационной безопасности и методология защиты информации / И. В. Аникин, В. И. Глова, Л. И. Нейман, А. Н. Нигматуллина // Учебное пособие. Казань: Изд-во Казан. гос. техн. ун-та, 2008 с. 358. [Електронний ресурс]. – Режим доступу: http://kai-t9-labs.googlecode.com/hg/tasks/MUCK3U/%D0%9C%D0%B8%D0%A1%D0%97%D0%9A%D0%98%20(%D1%83%D1%87%D0%B5%D0%B1%D0%BD%D0%BE%D0%B5%20%D0%BF%D0%BE%D1%81%D0%BE%D0%B1%D0%B8%D0%B5).pdf*
38. *Бодюл Є. М. Інформаційна безпека банку / Є. М. Бодюл // Протидія злочинам, які вчиняються з використанням комп'ютерних мереж [Текст]: тези доповідей Міжнародної науково-практичної конференції (м. Севастополь, 1–2 жовтня 2010 року) / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». – Суми : ДВНЗ «УАБС НБУ», 2010. – С.53-55.*
39. *Кібальник Л. О. Концептуальний підхід до формування інформаційної безпеки банківських установ в системі економічної безпеки [Електронний ресурс] / Л. О. Кібальник, І. Ю. Напора // Ефективна економіка. – 2016. – № 12. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=5303.*

4.3. ДЕРЖАВНА ПОЛІТИКА ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

КАРПОВА КРІСТІНА ВІКТОРІВНА, *к.е.н., доцент,*
професор кафедри управління безпекою,
правоохоронної та антикорупційної діяльності
Міжрегіональної Академії управління персоналом

На сьогодні в Україні адекватне реагування на загрози інформаційній безпеці виходить за межі чинної нормативної бази і можливе лише за умови прийняття політичних рішень компетентними органами. Необхідно визнати, що в умовах української демократії формування державної політики у будь-якому напрямі залежить не тільки від експертних оцінок та об'єктивного врахування національних інтересів, але й від політичної кон'юнктури у певний період [1].

При цьому важливо відзначити наявність певних нормативно-правових актів спрямованих на формування ефективного механізму забезпечення інформаційної безпеки держави. В якості такого механізму можна розглядати формалізований алгоритм дій взаємопов'язаних структурних та функціональних елементів системи, які забезпечують захист та розвиток інформаційного простору відповідно до національних інтересів.

У цьому механізмі повинні бути враховані національні інтереси в інформаційному середовищі, внутрішні та зовнішні загрози цим інтересам і передбачений комплекс засобів, які відносяться до підсистеми виявлення та нейтралізації загроз як складової системи інформаційної безпеки держави. При розв’язанні проблеми інформаційної безпеки держави необхідно виділяти систему інформаційної безпеки як функціональну систему, що відображає процеси взаємодії інтересів та загроз щодо їх відповідної реалізації й нейтралізації, а розвиток інформаційного суспільства дозволяє стверджувати про існування і функціонування певної системи забезпечення інформаційної безпеки. При цьому названа система забезпечення – це взаємопов’язана і взаємообумовлена сукупність відповідних організаційних структур, сил, засобів, а також певних процедур (правил) формування і реалізації

управлінських рішень в інформаційній галузі національної безпеки. Таким чином, реалізація системного підходу при дослідженні інформаційної безпеки зобов’язує вирізняти систему інформаційної безпеки та її складову – систему забезпечення інформаційної безпеки.

Забезпечення інформаційної безпеки передбачає першочерговий захист таких елементів системи: державних інформаційних ресурсів та іншої інформації з обмеженим доступом; комплексів, засобів і систем передавання, накопичення та зберігання інформації; інформаційного простору від поширення інформації, зміст якої суперечить національним інтересам держави.

У широкому розумінні до системи забезпечення інформаційної безпеки необхідно віднести Верховну Раду України, Президента України, зацікавлені міністерства, регуляторні та контролюючі державні органи, споживачів інформації та інших суб'єктів [1; 2].

У більш вузькому розумінні цих понять до елементів системи забезпечення інформаційної безпеки можна віднести:

- нормативно-правові акти, які регламентують суспільні відносини в інформаційній сфері та встановлюють юридичну відповідальність у випадку їх порушення;
- державні та недержавні організації, які забезпечують продукцією ринок інформаційних послуг (ЗМІ, інформаційні агенції, служби, аналітичні та дослідні організації, власники каналів електронного зв'язку, інтернет-провайдери, кіноіндустрія та індустрія розваг тощо);
- сукупність спеціально уповноважених центральних органів виконавчої влади та державного управління, які контролюють дотримання інформаційного законодавства;
- практичну діяльність визначених законами суб'єктів забезпечення інформаційної безпеки, що спрямована на розвиток вітчизняного інформаційного простору.

Правове регулювання у сфері інформаційної безпеки буде тією чи іншою мірою стосуватися закріплених у Конституції прав особи на інформацію,

положень про демократичний устрій, плюралізм думок тощо, законодавства про інформацію, про забезпечення національної безпеки, охорону державної та комерційної таємниці, діяльність ЗМІ, Інтернету, а також захист інформації з обмеженим доступом [1; 3].

Потребує вдосконалення нормативно-правова база загальнодержавної системи забезпечення інформаційної безпеки, особливо за такими важливими напрямами як встановлення порядку інформаційного обміну та забезпечення безумовного дотримання відповідальності посадових осіб, громадян за додержання вимог інформаційної безпеки. Також необхідно прискорювати налагодження двостороннього та багатостороннього співробітництва з міжнародними організаціями для спільного вирішення проблем правового гарантування інформаційної безпеки, розробки міжнародного законодавства в цій сфері. В основу такого співробітництва доцільно покласти нові підходи до законодавчого визначення порядку доступу інших держав або окремих громадян інших держав до національних інформаційних ресурсів України та порядку використання цих ресурсів на основі договорів з іншими державами, а також визначення порядку поширення та використання інформаційної продукції зарубіжного виробництва на території України. При цьому досить важливим є врахування вимог інформаційної безпеки при закупівлі зарубіжних програмно-технічних та телекомунікаційних засобів, їх використання в стратегічно важливих галузях, на об'єктах важливого державного та суспільного значення.

Першочерговими заходами щодо реалізації політики забезпечення інформаційної безпеки України є:

- розробка і впровадження механізмів реалізації правових норм, що регулюють відносини в інформаційній сфері, а також підготовка концепції правового забезпечення інформаційної безпеки України;
- розробка і реалізація механізмів підвищення ефективності державного керівництва діяльністю державних ЗМІ, здійснення державної інформаційної політики;

•прийняття і реалізація державних програм, що передбачають формування загальнодоступних державних інформаційних ресурсів, комплексну протидію інформаційним загрозам, забезпечення технологічної незалежності країни в галузі створення та експлуатації інформаційно-телекомунікаційних систем оборонного призначення;

•розвиток системи підготовки кадрів за напрямом – інформаційна безпека;

•приведення до однієї системи вітчизняних стандартів у галузі інформатизації і забезпечення інформаційної безпеки [2; 4].

Державна політика щодо забезпечення інформаційної безпеки України повинна реалізовуватися через відповідні форми і способи, які утворюють власне інструмент вирішення всього комплексу завдань із захисту життєво важливих інтересів особистості, суспільства та держави. Тому необхідне чітке юридичне оформлення при розробці нормативних актів, які регулюють діяльність органів інформаційної безпеки. Застосування тих чи інших форм і способів правового захисту залежить від того, чи є інформаційні загрози наслідком ненавмисних або навмисних дій суб'єктів інформаційного процесу. У першому випадку забезпечення інформаційної безпеки здійснюється відповідно у формах інформаційного захисту, патронату та інформаційної кооперації, у другому – у формі інформаційного протиборства [5].

При цьому захист життєво важливих інтересів фізичних і юридичних осіб від інформаційних загроз (інформаційний захист) досягається шляхом внесення в порядку законодавчої ініціативи законопроектів, здійснення судового захисту, проведення оперативних заходів силами і засобами інформаційної безпеки. Інформаційний патронат як форма забезпечення інформаційної безпеки цих осіб з боку держави припускає забезпечення органів управління системи інформаційної безпеки держави відомостями про дестабілізуючі фактори і загрози стану інформованості фізичних і юридичних осіб (інформаційне забезпечення інформаційної безпеки).

Отже інформаційне забезпечення інформаційної безпеки включає збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози,

їхню обробку, обмін інформацією між органами керування і силами та засобами системи інформаційної безпеки. Його основу складає збирання (добування) необхідних відомостей, здійснюване в процесі розвідувальної, контррозвідувальної, оперативно-розшукової і оперативно-інформаційної діяльності.

Водночас між рівноправними суб'єктами інформаційного процесу (фізичними, юридичними, міжнародними), який включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про дестабілізуючі фактори, інформаційні загрози та захист від них доступними законними способами і засобами використовується така форма забезпечення інформаційної безпеки як інформаційна кооперація [5; 6].

Для конкретної особистості такими способами і засобами можуть бути: судовий захист прав і свобод у використанні інформації; адміністративний захист її життєво важливих інтересів у інформованості з боку територіальних або відомчих органів інформаційної безпеки; автономний захист своїх прав і свобод в основному із застосуванням технічних засобів захисту, особистої, сімейної і професійної таємниці. Це ж характерно і для суспільних об'єднань, організацій (підприємств). Разом із тим, при наявності у них власних органів інформаційної безпеки, їхні можливості у сфері автономного захисту суттєво розширюються.

У зв'язку з усе більш активним використанням інформаційної сфери для розв'язання соціальних конфліктів останнім часом стає все більш актуальним використання інформаційного протиборства в якості форми забезпечення інформаційної безпеки. Заходи, що вживаються для забезпечення інформаційної безпеки повинні бути адекватними наявним і прогнозованим загрозам, причому вони можуть бути як пасивними, так і активними. На державному рівні такими конкретними заходами є інформаційна війна, яка ведеться з використанням політичних, дипломатичних, економічних, інформаційно-психологічних, інформаційно-технічних і воєнних способів. Основною формою інформаційної війни на державному рівні є спеціальна

інформаційна операція. Визначення мети операції, завдань, часу та місця проведення здійснюється воєнно-політичним керівництвом держави [5; 7].

Пасивне забезпечення інформаційної безпеки передбачає реагування на вже наявні загрози, спрямоване на безпосередню протидію акціям, що є деструктивними щодо соціальної системи. З цією метою створюється певна система захисту, яка складається з низки адміністративно-режимних, правових, фізичних, апаратно-технічних, програмних та інших заходів, які утворюють якби безперервну оболонку навкруги системи, що підлягає захисту. Міцність такої оболонки визначається міцністю найбільш слабкої її ланки. На відміну від пасивного, активне забезпечення інформаційної безпеки спрямоване на завчасне виявлення та попередження загроз. Це може досягатися шляхом проведення заходів, спрямованих на з'ясування планів, цілей, сил та засобів конфронтуючої соціальної системи, а також на протидію деструктивним акціям на етапі їхньої підготовки.

Політика забезпечення інформаційної безпеки України в першу чергу полягає у забезпеченні конституційних прав людини на доступ до інформації, використанні інформації в інтересах здійснення незабороненої чинним законодавством діяльності, фізичного, інтелектуального й духовного розвитку, а також у захисті інформації, яка стосується особистої безпеки громадянина та суспільства в цілому. В цьому контексті повинна передбачатися концентрація зусиль стосовно запобігання проявам інформаційно-диверсійної діяльності терористичних організацій, груп, окремих осіб, спрямованих на дестабілізацію суспільного життя в країні та завдання шкоди громадянам, державі.

Водночас основні заходи цієї політики необхідно спрямовувати на створення належних умов забезпечення конфіденційності, цілісності та гарантованого адресного доступу до важливої для держави, особи й суспільства інформації, а також надійної нейтралізації діяльності іноземних політичних, економічних, військових, розвідувальних структур, спрямованих проти інтересів України. Крім окреслених заходів в інтересах повноцінного функціонування системи забезпечення інформаційної безпеки держави

необхідно створити відповідну матеріально-технічну базу, організувати високоефективну науково-практичну роботу та підготовку професійних кадрів.

Суб'єктом національних інтересів повинен виступати саме український народ, який реалізує свої інтереси у відповідності зі встановленими Конституцією та законами України правами та обов'язками.

Для формування певного національного інтересу необхідний пошук балансу між інтересами народу або нації та інтересами окремої людини. Оскільки легальність цього національного інтересу обумовлюється його відповідністю нормам міжнародного та національного законодавства та його реалізації за допомогою законних методів, то баланс між інтересами нації та окремої людини так само обумовлюється балансом між правами нації та правами людини. Вимога наявності комплексного підходу та досягнення консенсусу щодо визначення конкретних національних інтересів, передбачає врахування багатьох політико-правових, економічних, історичних, моральних факторів. Основою національних інтересів є триєдина система, що включає в себе національну ідею, головні цілі та прагнення (потреби) суспільства. [8; 9].

Національні стратегічні цілі України є проекцією пріоритетних національних інтересів її розвитку, які визначаються передусім необхідністю захисту суверенітету і незалежності України, забезпечення непорушності її кордонів та територіальної цілісності, створення умов для забезпечення прав і свобод людини, демократичного розвитку та економічного процвітання держави, як основи зростання добробуту її громадян, захисту та подальшого розвитку духовних цінностей [10]. Вони спрямовані на виконання наступних стратегічних завдань в інформаційній сфері:

- неухильне забезпечення принципів свободи слова, висловлення поглядів, безперешкодного доступу громадян до інформації, політичного плюралізму, недопущення будь-яких рецидивів політичної цензури та перешкоджання професійній діяльності журналістів – пріоритетні завдання державної інформаційної політики;

•реальне забезпечення прав громадян на вільний обмін і передачу інформації, створення можливостей отримання об'єктивної інформації з різних джерел, захист національного інформаційного простору від зазіхань на державні інтереси та моральні підвалини суспільства [6, 14].

Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що являє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, поширення і використання інформації, а також регулювання суспільних відносин. Інформаційна сфера, будучи системоутворюючим фактором життя суспільства, активно впливає на стан всіх складових національної безпеки України. Національна безпека істотно залежить від забезпечення інформаційної безпеки, і в ході технічного прогресу ця залежність буде зростати. [4; 12].

В інформаційній сфері *національні інтереси* полягають:

•особистості – у реалізації конституційних прав людини і громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку, а також у захисті інформації, що забезпечує особисту безпеку;

•суспільства – у забезпеченні інтересів особистості в цій сфері, зміцненні демократії, створенні правової соціальної держави, досягненні і підтримці суспільної згоди, у духовному відновленні держави та національної ідентичності;

•держави – у створенні умов для гармонічного розвитку інформаційної інфраструктури, для реалізації конституційних прав і свобод людини і громадянина в області одержання інформації і користування нею з метою забезпечення непорушності конституційного ладу, суверенітету і територіальної цілісності України, політичної, економічної і соціальної стабільності, у безумовному забезпеченні законності і правопорядку, розвитку рівноправного і взаємовигідного міжнародного співробітництва [4; 5].

На основі національних інтересів України в інформаційній сфері формуються стратегічні і поточні задачі внутрішньої і зовнішньої політики

держави щодо забезпечення інформаційної безпеки. Виділяються чотири основні складові національних інтересів України в інформаційній сфері.

Перша складова включає дотримання конституційних прав і свобод людини і громадянина в області одержання інформації і користування нею, забезпечення духовного відновлення Української держави, збереження і зміцнення моральних цінностей суспільства, традицій патріотизму і гуманізму, культурного і наукового потенціалу країни [4].

Для реалізації окресленого напряму цінностей та досягнення базового європейського рівня їх забезпечення потрібно:

- підвищити ефективність використання інформаційної інфраструктури в інтересах розвитку, консолідації суспільства, духовного відродження української національної ідентичності;
- удосконалити систему формування, збереження і раціонального використання інформаційних ресурсів, що складають основу науково-технічного і духовного потенціалу нації та держави в цілому;
- забезпечити конституційні права і свободи людини і громадянина вільно шукати, одержувати, передавати, робити і поширювати інформацію будь-яким законним способом, одержувати достовірну інформацію про стан навколишнього середовища;
- гарантувати виконання конституційних прав і свобод людини і громадянина на особисту і сімейну таємницю, таємницю листування, телефонних переговорів, поштових, телеграфних та інших повідомлень, на захист своєї честі і свого доброго імені, з одночасною забороною збору, збереження, використання і поширення інформації про приватне життя особи без її згоди та іншої інформації, доступ до якої обмежений законодавством;
- зміцнити механізми правового регулювання відносин в області охорони інтелектуальної власності, створити умови для дотримання встановлених у правовому просторі обмежень на доступ до конфіденційної інформації;

•гарантувати свободу масової інформації, не допускаючи антидержавної пропаганди й агітації, спрямованої на розпалення соціальної, расової, національної чи релігійної ненависті й ворожнечі [4; 12].

Друга складова національних інтересів в інформаційній сфері пов’язана із забезпеченням доступу громадян та громадських організацій до відкритих державних інформаційних ресурсів та надання інформації про діяльність органів державної влади. Вона містить у собі інформаційно-пропагандистське супроводження й інформаційне забезпечення державної політики, спрямованої на гарантоване доведення до української і міжнародної громадськості достовірної інформації про Україну [4].

Для досягнення цих намічених цілей потрібно:

•зміцнювати державні ЗМІ, розширювати їхні можливості по своєчасному доведенню достовірної інформації до українських та іноземних громадян;

•активно використовувати популярні комерційні (українські та зарубіжні) ЗМІ, власниками яких є громадяни України, в інформаційно-пропагандистських цілях при формуванні позитивного міжнародного іміджу нашої держави;

•інтенсифікувати формування відкритих державних інформаційних ресурсів, підвищити ефективність їхнього господарського використання [4].

Третя складова національних інтересів в інформаційній сфері містить у собі розвиток сучасних інформаційних технологій, вітчизняну індустрію інформації, у тому числі виробництво засобів інформатизації, телекомунікації і зв'язку, забезпечення потреб внутрішнього ринку її продукцією і вихід цієї продукції на світовий ринок, а також забезпечення накопичення, збереження й ефективного використання вітчизняних інформаційних ресурсів. На такій основі можна вирішувати проблеми створення сучасних наукомістких технологій, технологічного переозброєння промисловості, збільшення досягнень вітчизняної науки і техніки перш за все в інформаційній сфері. Україна повинна зайняти гідне місце серед світових лідерів по розробці та впровадженню нових інформаційних технологій в галузі мікроелектронної і комп'ютерної промисловості [4; 12].

Для реалізації визначених цінностей та досягнення світового рівня їх забезпечення потрібно:

•розвивати та удосконалювати інформаційну інфраструктуру держави за рахунок підтримки вітчизняної індустрії інформаційних послуг і підвищення ефективності та якості використання державних інформаційних ресурсів;

•забезпечити державну підтримку вітчизняних фундаментальних і прикладних досліджень, розробок у сферах інформатизації, телекомунікації і зв'язку для випереджувального розвитку національного виробництва конкурентноздатних засобів і систем інформатизації, телекомунікації та зв'язку, а також розширювати участь України в міжнародній кооперації виробників цих засобів і систем.

Четверта складова національних інтересів в інформаційній сфері містить у собі повноцінний та належний захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки інформаційних і телекомунікаційних систем. Інформаційний простір України законодавчо захищатиметься, в першу чергу від пропагування антидержавних ідей, міжнаціональної та міжконфесійної ворожнечі, насилля, ненависті, аморальності та інших дій, несумісних з інтересами особистості, суспільства і держави [4].

У цих цілях необхідно:

•забезпечити перехід від виключно організаційних методів до застосування високотехнологічних засобів безпеки інформаційних систем, включаючи мережі зв'язку, насамперед безпеку первинних мереж зв'язку та інформаційних систем органів державної влади, фінансово-кредитної і банківської сфер, сфери господарської діяльності, а також систем і засобів інформатизації озброєння та військової техніки, систем керування військами і зброєю, екологічно небезпечними й економічно важливими виробництвами;

•інтенсифікувати розвиток вітчизняного виробництва спеціалізованих апаратних і програмних комплексів та засобів захисту інформації і методів контролю за їхньою ефективністю;

•забезпечити надійний захист національних інформаційних ресурсів і в першу чергу даних, що складають державну таємницю;

•розширювати міжнародне співробітництво України в галузі формування і безпечного використання інформаційних ресурсів, протидії загрозі розв'язання міждержавного інформаційного протиборства, особливо в суміжних з Україною країнах [4].

У Законі України «Про основи національної безпеки України» визначені такі пріоритети національних інтересів України (без прив`язки до конкретних сфер):

•гарантування конституційних прав і свобод людини і громадянина;

•розвиток громадянського суспільства, його демократичних інститутів;

•захист державного суверенітету, територіальної цілісності та недоторканності державних кордонів, недопущення втручання у внутрішні справи України;

•зміцнення політичної і соціальної стабільності в суспільстві;

•забезпечення розвитку і функціонування української мови як державної в усіх сферах суспільного життя на всій території України, гарантування вільного розвитку, використання і захисту російської, інших мов національних меншин України;

•створення конкурентоспроможної, соціально орієнтованої ринкової економіки та забезпечення постійного зростання рівня життя і добробуту населення;

•збереження та зміцнення науково-технологічного потенціалу, утвердження інноваційної моделі розвитку;

•забезпечення екологічно та техногенно безпечних умов життєдіяльності громадян і суспільства, збереження навколишнього природного середовища та раціональне використання природних ресурсів;

•розвиток духовності, моральних засад, інтелектуального потенціалу українського народу, зміцнення фізичного здоров’я нації, створення умов для розширеного відтворення населення;

•інтеграція України в європейський політичний, економічний, правовий простір та в євроатлантичний безпековий простір;

•розвиток рівноправних взаємовигідних відносин з іншими державами світу в інтересах України [13].

Звісно, що реалізація кожного із зазначених пріоритетів потребує специфічного інформаційного забезпечення і супроводження, а головне створення ефективного механізму звітності органів державної влади та їх окремих представників, державних службовців перед громадськістю, у тому числі й через засоби масової інформації. В цьому контексті найважливішим завданням державної інформаційної політики вважається створення умов правової і фінансової незалежності ЗМІ. Незалежність ЗМІ дає можливість їм виступати захисниками інтересів громадян та громадських організацій.

Практична реалізація державної інформаційної політики у всіх її функціональних і тимчасових аспектах потребує розвитку інформаційного законодавства як системи взаємопогоджених правових норм, що базуються на конституційних принципах устрою держави.

Тому норми права інформаційного законодавства присутні в більшості законодавчих актів України. Інформаційне законодавство, що включає нормативно-правові акти, які цілком присвячені питанням правового регулювання в інформаційній сфері, і окремі норми за даним предметом в інших нормативно-правових актах, є одночасно основним інструментом реалізації та однією з головних сфер формування державної інформаційної політики. На цей час уже прийнято і діє ряд базових законів, але процес формування інформаційного законодавства проходить досить повільно, хоча достатньо широке коло правових відносин в інформаційній сфері так і залишилося неурегульоване [14; 15].

У зв'язку з цим є необхідність формулювання певних напрямів розробки інформаційного законодавства України, зокрема можна запропонувати такі:

•забезпечення інформаційної безпеки держави, суспільства, громадянина та першочерговий захист прав громадян в умовах переходу до інформаційного

суспільства;

•функціональне поєднання прав юридичних і фізичних осіб на інформацію з відповідальністю за правопорушення в сфері інформації та інформатизації;

•забезпечення захисту інтелектуальної власності на інформацію та правове визначення порядку формування інформаційних ресурсів в умовах рівності всіх форм власності і ринкової економіки.

В якості першочергового завдання можна вважати розробку комплексної програми розвитку інформаційного законодавства. Пріоритети цієї програми повинні змінюватися відповідно до динаміки об'єктивних змін поточних пріоритетів в державній інформаційній політиці. Іншим перспективним, актуальним і своєчасним є завдання щодо створення проекту інформаційного кодексу України, а в кінцевому рахунку – формування високої інформаційно-правової культури громадян.

Цими проблемами держава повинна займатися на рівні основного напрямку діяльності, приділяючи їм увагу і докладаючи для їх вирішення значних зусиль. В першу чергу необхідно визнати і реально здійснювати як самостійну і основну таку спеціальну внутрішньодержавну функцію, як інформаційну. На сьогодні така функція реалізується державою в рамках функції політичного управління.

Наявна в нашій державі нормативно-правова база забезпечення інформаційної безпеки нечисельна. В основному – це відомчі або специфічні нормативні акти, що стосуються окремих сфер діяльності держави, суспільства або особистості. При цьому до основних, в певній мірі функціонально-профільних, нормативно-правових актів можна віднести Закони України «Про основи національної безпеки України» [13] та «Про інформацію» [16].

Зокрема Закон України «Про інформацію» закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності, а також стверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в галузі інформації [16]. Крім того Закон встановлює загальні правові основи одержання, використання, поширення та

зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації

Всім громадянам України, юридичним особам і органам державної влади гарантується право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій. Також кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України.

Визначено, що державну інформаційну політику розробляють і здійснюють органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції. Як недолік такого законодавчого підходу можна назвати недоцільність узагальненого визначення розробників ДІП одночасно й тими хто її реалізує, а також відсутність державних структур відповідальних за періодичне уточнення інформаційної політики та документальне доведення основних її засад до суспільства.

У другому розділі Закону визначено основні напрями та види інформаційної діяльності – це одержання, використання, поширення та зберігання інформації. Надаються визначення цих напрямів інформаційної діяльності, зокрема одержання – це набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою. Використання – це задоволення інформаційних потреб громадян, юридичних осіб і держави. Поширення – це розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошуваної інформації. Зберігання – це належний стан інформації та її матеріальних носіїв [16].

У наступних розділах наведені галузі, види джерела інформації та режими доступу до неї, визначені учасники інформаційних відноси, їх права та обов`язки. Основними учасниками цих відносин є: автори, споживачі, поширювачі, зберігачі (охоронці) інформації.

Також визначено, що держава гарантує всім учасникам інформаційних відносин рівні права і можливості доступу до інформації. Заборонено цензуру та втручання в професійну діяльність журналістів і засобів масової інформації з боку органів державної влади або органів місцевого самоврядування, їх посадових осіб. Інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання расової, національної, релігійної ворожнечі, посягання на права і свободи людини.

Окремий розділ Закону присвячено міжнародній інформаційній діяльності, співробітництві з іншими державами, зарубіжними і міжнародними організаціями в галузі інформації. Міжнародне співробітництво в галузі інформації з питань, що становлять взаємний інтерес, здійснюється на основі міжнародних договорів, укладених Україною та юридичними особами, які займаються інформаційною діяльністю.

Слід розуміти, що в сучасній динамічній ситуації неможливо забезпечити інформаційну безпеку держави лише регламентацією інформаційної сфери, оскільки нові виклики потребують адекватних відповідей, в зв’язку з чим особливого значення набуває механізм створення нової інформації, конкуренція та багатоманітність джерел цієї інформації. Саме тому, для забезпечення інформаційної безпеки особливо важливим є дотримання принципів прозорості в інформаційній сфері та доступності різноджерельної інформації. Також важливим напрямом забезпечення інформаційної безпеки є законодавче регулюванню цієї сфери [15].

Відповідно до зазначеного вище, Закон України «Про основи національної безпеки України» являє собою довідник визначень, що стосуються інформаційної безпеки. Зокрема перераховано об’єкти, суб’єкти інформаційної

безпеки, підстави гарантування державою цілісності інформаційного простору, загрози інформаційному простору і інформаційній безпеці (не розрізняючи їх та не передбачаючи можливості виникнення нових загроз). Крім того більш загальними фразами перераховано шляхи забезпечення інформаційної безпеки України, визначено основні напрями державної інформаційної політики та інформаційної безпеки, точніше, напрямки державної політики в інформаційній сфері [13].

Водночас за оцінкою вітчизняного вченого Б.А. Кормича у вищезгаданому законі всі види безпеки, в тому числі й інформаційна, пов'язуються зі станом захищеності життєво важливих інтересів її об'єктів, причому об'єктами називаються: людина і громадянин – їхні конституційні права і свободи; суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси; держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність [8].

Одночасно у Концепції національної програми інформатизації, інформаційна безпека називається невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. А об'єктами інформаційної безпеки визначаються інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни [6; 8].

Загалом, в Законі систематизовані і наведені повноваження Президента України, Верховної Ради України, Ради національної безпеки і оборони України, Кабінету Міністрів України, міністерств, Служби безпеки України, інших центральних органів виконавчої влади, місцевих державних адміністрацій, органів місцевого самоврядування, правоохоронних органів, судів загальної юрисдикції, Генеральної прокуратури України; окремі права громадян в інформаційній сфері. Очевидно, що закріплення таких норм, які відтворюють вже законодавчо закріплені повноваження в інформаційній сфері

не лише не врегульовує відповідні суспільні відносини, але й створює можливість обмеження їх діяльності в сфері інформаційної безпеки цими повноваженнями.

Слід зазначити, що переважна більшість статей Закону носить бланкетний характер і відсилає до норм чинного законодавства, що аж ніяк не сприяє визначеності правового регулювання. У цьому контексті статті, присвячені правовому регулюванню інформаційної безпеки фактично спрямовані на закріплення рамкових засад цієї категорії та є переважно декларативними. Відсутність конкретизації і орієнтація на загальні положення більш прийнятна для концепції інформаційної безпеки а не для закону. Складність і багатоманітність інформаційних відносин передбачає необхідність систематизації нормативно-правових актів у інформаційній сфері, що можливо віднайде свою реалізацію в Інформаційному кодексі.

Саме у розвиток цього закону, мають бути розроблені документи наступного рівня, – нова Доктрина інформаційної (у т.ч. кібернетичної) безпеки, концепції, стратегії, програми за певними напрямами, які мають в цілому скласти основу правового регулювання інформаційної сфери.

Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою визначають рівень і темпи соціально-економічного, науково-технічного і культурного розвитку держави. За сучасних умов інформаційна складова набуває дедалі більшої ваги і стає одним з найважливіших елементів забезпечення національної безпеки України [17; 18].

Загалом основні принципи, норми та положення прийнятих законів сьогодні вже відповідають загально прийнятим міжнародно-правовим стандартам, міжнародним конвенціям з прав людини. Разом з тим, існування такої системи законодавчих актів ще не гарантує реального захисту інтересів суспільства щодо отримання вільної та неупередженої інформації.

Політика інформаційної безпеки держави реалізується в процесі діяльності як органів державної влади, так і недержавних інституцій. Ми можемо

стверджувати, що політика інформаційної безпеки визначає зміст діяльності держави та її компетентних органів, що охоплюється відповідними аспектами інформаційної функції держави та функції національної безпеки. На сьогоднішній день значення інформаційної діяльності держави значно розширилось, навіть важко скласти чіткий перелік сфер суспільного і державного життя, на які мають вплив результати цієї діяльності: це і права людини, військова та державна безпека, економіка, культура, внутрішня та зовнішня політика тощо. Взагалі, розглядаючи проблему просторового буття держави, потрібно зазначити, що воно виходить за рамки державних кордонів. Якщо мова йде про геополітичні інтереси, про сфери впливу і т. д., то ці аспекти діяльності державного апарату виходять далеко за межі території окремої держави [8; 19].

Отже, можна стверджувати, що основні напрямки політики інформаційної безпеки фактично формують державно-правовий механізм її реалізації. При цьому створення нормативно-правових актів, що регулюють відповідні суспільні відносини в інформаційній сфері, встановлюють міру поведінки та відповідальність суб'єктів інформаційних правовідносин лежить в основі його правової складової. Загальновідомо про абсолютну неможливість обмежувати державну діяльності суто внутрішньою або зовнішньою спрямованістю. Тому інституціональна складова механізму формування політики інформаційної безпеки включає існуючі внутрішньодержавні та міжнародні інституції, а також передбачає створення нових. Застосування в процесі діяльності державних інституцій конкретних, встановлених правовими нормами форм, способів і шляхів державного впливу на інформаційну сферу формує організаційну складову цього механізму.

Визначаючи місце політики інформаційної безпеки в системі діяльності держави по виконанню своїх функцій, треба сказати, що на сучасному етапі виникає необхідність розглядати в комплексі предмет і зміст діяльності держави та засоби і способи, що її забезпечують. Це означає перехід від використання поняття функції держави до такого поняття, як державна

політика, оскільки поняття функції держави розкриває лише одну із складових державної політики.

Політика являє собою організаційну та регулятивно-контрольну сфери суспільства, основні в системі інших сфер і такі, що охоплюють відносини та діяльність суб'єктів і об'єктів. Державна політика визначає зміст державної діяльності, способи її організації. Саме політика передбачає врахування та пов'язування інтересів держави з інтересами інших держав, соціальних груп та індивідів, і головне – визначення конкретного змісту та форм діяльності держави в тій чи іншій сфері [10; 20].

Разом з тим сама по собі політика є надправовою категорією і регулюється правовими нормами лише у своєму зовнішньому, формалізованому вираженні. Але конкретний зміст політики, особливо державної, являє собою волю держави, спрямовану на досягнення конкретної мети. Ця воля держави закріплюється у правових нормах, здійснюється за їх допомогою у процесі діяльності державних органів та інститутів. Таким чином, з правової точки зору існує певний механізм формування і реалізації державної політики, в сфері інформаційної безпеки це державно-правовий механізм інформаційної безпеки [8].

Державно-правовий механізм інформаційної безпеки являє собою сукупність державних інституцій, задіяних у процесі формування і впровадження цієї політики, їх ролі та відносин, що підпорядковані чіткій ієрархії правових норм і принципів. Цей державно-правовий механізм, відповідно до означених нами напрямків реалізації політики інформаційної безпеки, складається з трьох взаємопов'язаних елементів [6; 8].

По-перше, це сукупність державних інституцій, задіяних у процесі формування і впровадження політики інформаційної безпеки, тобто інституціональний механізм інформаційної безпеки.

По-друге, це сукупність ролей та відносин, які включають правові відносини, що виникають при проведенні такої політики, та специфічні ролі, форми і методи діяльності суб'єктів проведення політики інформаційної

безпеки, тобто організаційний, або навіть можна сказати управлінський механізм інформаційної безпеки.

По-третє, це ієрархічна сукупність правових норм та принципів, які регулюють зміст та процес проведення цієї політики, тобто правовий механізм інформаційної безпеки.

Ефективність захисту інформаційної безпеки держави в цілому забезпечується ефективністю кожної складової її механізму.

Зважаючи на зазначене вище, можна акцентувати увагу на загальних методах функціонального забезпечення державно-правового механізму інформаційної безпеки держави, які в свою чергу розділяються на правові, організаційно-технічні й економічні.

При цьому до правових методів забезпечення інформаційної безпеки відноситься розробка нормативних правових актів, що регламентують відносини в інформаційній сфері, і нормативних методичних документів з питань забезпечення інформаційної безпеки України. За рахунок застосування організаційно-технічних методів забезпечення інформаційної безпеки формуються організаційна та функціональна складові системи забезпечення інформаційної безпеки України.

Розробка програм забезпечення інформаційної безпеки України і визначення порядку державного фінансування їх впровадження проводиться за рахунок економічних методів забезпечення інформаційної безпеки України. Крім того здійснюється удосконалення механізму фінансування заходів захисту інформації, створення системи страхування інформаційних ризиків фізичних і юридичних осіб.

Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що являє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, поширення і використання інформації, а також регулювання суспільних відносин. При цьому окреслено конкретні умови при виконанні яких інформаційна сфера в нашій державі стане одним із системоутворюючих факторів життя суспільства

та суттєво впливатиме на стан політичної, економічної, оборонної та інших складових національної безпеки України.

Взаємозв'язок між життєво важливими національними інтересами в інформаційній сфері особи, суспільства й держави та реалізацією основних засад державної інформаційної політики конкретизовано шляхом виділення та детального розгляду цілей досягнення кожної з основних складових національних інтересів. На основі національних інтересів України в інформаційній сфері формуються стратегічні і поточні задачі внутрішньої і зовнішньої політики держави щодо забезпечення інформаційної безпеки.

Зазначене підтверджує доктринальне визначення інформаційної безпеки як невід'ємної складової кожної зі сфер забезпечення національної безпеки і водночас важливої самостійної сфери національної безпеки України.

Також важливим напрямом забезпечення інформаційної безпеки є законодавче регулюванню цієї сфери, що підкреслює важливість розробки комплексної програми розвитку інформаційного законодавства. Важливим етапом реалізації цієї програми стане створення проекту Інформаційного кодексу України, а в кінцевому рахунку – формування високої інформаційно-правової культури суспільства й кожного громадянина держави.

З правової точки зору можна стверджувати про існування певного механізму формування і реалізації державної політики, в сфері інформаційної безпеки – це державно-правовий механізм інформаційної безпеки, тобто сукупність державних інституцій, задіяних у процесі формування і впровадження цієї політики, їх ролі та відносин, що підпорядковані чіткій ієрархії правових норм і принципів.

Список використаних джерел:

1. *Толубко В.Б., Рось А.О. Складові інформаційної боротьби // Наука і оборона. – 2002. – №2.*
2. *Бекетов Н.В. Информационная безопасность развития государства // Информационные ресурсы России. – 2006. – № 6. – С. 34.*
3. *Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. – К.: Кондор, 2004. – 384 с.*
4. *Богданович В.Ю. Інформаційна безпека України і шляхи її забезпечення. – К.: "Основа", 2003. – 186 с.*

5. *Богуш В.М., Юдін О.К. Інформаційна безпека держави. – К.: "МК-Прес", 2005. – 432 с.*
6. *Ліпкан В.А. Національна безпека України: нормативно-правові аспекти забезпечення. – К.: Текст, 2003. – 180 с.*
7. *Литвиненко О.В. Проблеми забезпечення інформаційної безпеки у сучасному світі. – К.: ІМВ КНУ ім. Т. Шевченка, 1996. – 90 с.*
8. *Ковалева М.С. Зволюция понятия риска // Социологическое обозрение. – 2002. – № 1. – С. 18-21.*
9. *Ожеван М.А., Недбаєвський С.Л., Дубов Д.В. Індикатори реальних загроз національній безпеці України в інформаційній сфері // Стратегічна панорама. – № 1.– 2008. – С. 126-129.*
10. *Соснін О.В. Проблеми державного управління системою національних інформаційних ресурсів з наукового потенціалу України: Моног. – К.:Інст. держави і права ім. В. Корецького НАН України, 2003. – 572 с.*
11. *Зинченко А.С. Об информационной политике в Украине // Событие. 2000. №42.*
12. *Богданович В.Ю. Теоретические основы анализа проблем национальной безопастности государства в военной сфере.: Монограф. – К.: "Основа", 2006. – 296 с.*
13. *Закон України "Про інформацію" // Відомості Верховної Ради. – 1992. – № 48, ст. 650-651.*
14. *Закон України "Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015роки" // Відомості Верховної Ради України. – 2007. – № 12.*
15. *Ліпкан В.А. Безпекознавство: Навч. посібник. – К. – Вид-во Європейського університету, 2003. – 208 с.*
16. *Закон України "Про Раду національної безпеки і оборони України" від 5 березня 1998 року // Відомості Верховної Ради України. – 1998. –№35. – с. 237.*
17. *Закон України "Про захист інформації в автоматизованих інформаційних системах" // Відомості Верховної Ради. – 1994. – № 31, ст. 286.*
18. *Стратегії розвитку України: теорія і практика // За ред. О. С. Власюка. – К. : НІСД, 2002. – 864 с.*
19. *Расторгуев В.П. Философия информационной безопасности. - М., 2003. – 186 с.*
20. *Соснін О.В., Корнейко О.В., Шестак І.М. Проблеми розвитку комунікацій у контексті їх безпеки // Стратегічна панорама. – 2009. – № 1. – С.172-178.*

4.4. АДМІНІСТРАТИВНО-ПРАВОВІ КОНЦЕПТИ КОРПОРАТИВНИХ МОДЕЛЕЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

ЛИСЕНКО СЕРГІЙ ОЛЕКСІЙОВИЧ, *к.ю.н., доцент,*
доцент кафедри управління безпекою,
правоохоронної та антикорупційної діяльності
Міжрегіональної Академії управління персоналом

Моделювання використовується в науці і практиці, коли пряме дослідження фактів неможливо або недоцільно.Різноманіття завдань наукової та практичної діяльності породжує і різноманіття видів і способів моделювання. Так, для вирішення архітектурних і містобудівних завдань, конструювання машин, літаків, створення нових зразків товарів масового споживання застосовується моделювання зовнішніх форм об'єктів.

У галузі правових наук, слідчій і судовій практиці моделювання теж відомо не перший день. Однак, стосовно до забезпеченням інформаційної безпеки взагалі, освоєння цього методу проходить повільно.

Сьогодні терміни «модель», «правова модель», «модель праворозуміння», «модель правового регулювання», «модель юридичного процесу», «модельне законодавство» та інші є достатньо поширеними та вживаними в термінологічному обігу правознавства, проте при цьому розуміння моделі різними дослідниками вельми неоднозначно і досить невизначено місце категорії «правова модель». У зв'язку з цим виникає потреба в додатковому загальноправовому аналізі зазначеної категорії.

Необхідність в новому зверненні до питання про моделі в праві продиктована ще однією обставиною. Якщо стосовно природничих галузей знання вживання терміна «модель» і його смисловий зміст визначені і зрозумілі, як з позиції структурно-логічного чи системного аналізу, то в області гуманітарного знання, і, зокрема, юриспруденції, використання різного роду моделей вимагає ґрунтовної теоретичної бази.

У зв'язку з цим, вважаємо доцільним провести узагальнення підходів до розуміння правової моделі інформаційної безпеки, аналіз її ознак і розробки операціонального визначення. Доречним є уточнення і узагальнення класифікацій правових моделей інформаційної безпеки, розгляд співвідношення категорії «правова модель» із суміжною до неї категорією «правова модель інформаційної безпеки» [1].

Слід констатувати відсутність досліджень з приводу форм реалізації правових моделей в законодавстві, зокрема щодо забезпечення інформаційної безпеки соціальних систем. Не в достатній мірі проаналізовано правові моделі забезпечення інформаційної безпеки, а також особливості застосування моделювання в процесі правопознанія.

Соціальна значущість нашого наукового наміру полягає в необхідності визначити адміністативно-методологічні засади та цінності застосування саме правових моделей в пізнанні закономірностей розвитку правових і соціальних явищ в феноменології безпеки, як держави в цілому, так і її окремих інституцій – соціальних систем.

В аспекті моделювання можуть бути розглянуті і більш загальні пізнавальні процедури, планування розслідування і побудова моделей дій співробітників безпеки з охорони інформації. Безумовно, не можна зводити процес розслідування тільки до моделювання. Мова може йти про особливий підхід до вивчення і опису явищ, деяких сторін розумової діяльності осіб, які забезпечують безпеку. Наше завдання створити і впровадити такі моделі дій субєктів інформаційної безпеки, якіб забезпечували безумовні і злагоджені їх дії під час організації самої системи інформаційної безпеки. Поряд із цим, необхідно створити і впровадити моделі діяльності для забезпечення самої процедури обігу та охорони інформації. Разом із цим виникає необхідність в провадженні моделей для обміну інформацією та розслідування фактів витоку, крадіжки та знищення інформації. Одночасно з цим слід приділити увагу створенню моделей для профілактики правопорушеннь та уникнення, тобто

стримання, можливих дій конкурентів направлених на інформаційне приниження нашого підприємтсва.

Феноменологічно близьким до поняття правового моделювання може бути поняття правового забезпечення інформаційної безпеки. Згідно аналізу першоджерел, його можна розглядати, як певний адміністративно-правовий режим, тобто такий, що врегульований правом і має нормативний характер щодо структур державного управління, порядок здійснення діяльності, що підлягає адміністративній конкретизації в процесі його реалізації.

Норми, які регламентують правове забезпечення інформаційної безпеки в такому сенсі доречно розглядати, як певний правовий регуляторний інститут міжгалузевого (комплексного) характеру, які регулюють суспільні відносини щодо захисту національних інтересів в інформаційній сфері (життєво важливих інтересів особистості, суспільства і держави на збалансованій основі) від загроз в умовах інформаційних загроз та критичних ситуацій.

Узагальнюючи дослідження провідних науковців, в якості функцій правової моделі інформаційної безпеки можна визначити наступні: програмуюча, описова, демонстраційна, перетворювальна, критеріальна, організаційно-проективна [2].

Незважаючи на відмінності в підході дослідників до опису моделювання, можна констатувати, що його сутність розуміється так, що для вивчення якого-небудь об'єкта (процесу, явища) використовується не сам об'єкт, а замінююча його модель. Така модель є засобом отримання інформації про об'єкт - оригінал, замінює його при постановці дослідів і в інших пізнавальних процедурах.

Під моделлю розуміється така, яка надається або матеріально реалізована, система, яка, відображаючи або відтворюючи об'єкт чі явища дослідження, здатна замінити його так, що її вивчення дає нам нову інформацію про цей об'єкт. Користуючись цією концепцією, ми акцентуємо увагу на основних видах моделювання (уявному та матеріально-реалізованому). Ці моделі використовуються в теоретичній роботі і становлять практичний інтерес в

системному підході до цього методу, що дозволяє розділити на окремі елементи об'єкти - оригінали та модель, і вивчати характер зв'язків між ними, а потім дослідити відносини моделі і оригіналу, а також відносини моделі та інших суб'єктів відносин. Так само моделі дають можливості відображати або відтворювати за допомогою моделей об'єкт або окремі сторони об'єкта (процесу, явища), можливості отримувати в результаті вивчення моделі нову інформацію, тобто на можливість моделі бути джерелом інформації, яка в подальшому послужить підставою для виробництва висновків.

Під моделюванням систем інформаційної безпеки, як правило, розуміють відтворення характеристик деякої системи інформаційної безпеки, за допомогою інших об'єктів, спеціально створених для його вивчення [3, с. 97]. Цей останній об'єкт і зветься моделлю. На думку О. В. Мангушева [4, моделювання - це процес побудови моделі, яка необхідна: 1) для того, щоб зрозуміти, як влаштований конкретний об'єкт (його структура, основні властивості, закони розвитку і взаємодії з навколишнім світом); 2) для того, щоб навчитися управляти об'єктом (або процесом) і визначити найкращі способи управління при заданих цілях і критеріях; 3) для того, щоб прогнозувати прямі і непрямі наслідки реалізації заданих способів і форм впливу на об'єкт. Наведене визначення вченого цілком відповідає методології нашого дослідження, оскільки інформаційна безпека, опосередкована професійним мисленням, розглядається нами як динамічне утворення.

Моделювання набуває особливого значення при вивченні об'єктів, недоступних прямому спостереженню. «Моделювання – відзначає В. Г. Афанасьєв, - припускає наявність чітких методологічних і теоретичних передумов. Вихідною основою моделювання є матеріальна єдність світу, закономірностей його розвитку, згідно з якими якісно різним системам властиві аналогічні структурні і функціональні, закономірності, закони організації» [5, с. 157].

Як стає зрозумілим з аналізу наукової літератури моделювання характеризують такі основні принципи: 1) принцип аналогії та тотожності

моделі та об'єкта дослідження(системи інформаційної безпеки підприємтсв); 2) принцип взаємодії в процесі моделювання інтуїтивно-змістовних і формальних методів; 3) принцип отримання нового знання про об'єкт дослідження; 4) принцип експериментальної перевірки нового знання і деяких гіпотетичних уявлень про об'єкти певного роду; 5) принцип суперечливості інтуїтивно-змістовного і формального методів вивчення об'єктів; 6) принцип обмеження безлічі відносин об'єкта з іншими об'єктами та із зовнішнім середовищем; 7) різноманітність вибору моделей, як принцип моделювання, що відображає динаміку об'єкта; 8) принцип наявності нового знання про об'єкт; 9) принцип емпіричних доказових гіпотетико-інтуїтивних уявлень, покладених в основу побудови моделі; 10) принцип представлення моделі, як опосередкованої ланки між об'єктом дослідження і суб'єктом (дослідником) [3].

В цілому, слід зазначити, що моделювання, за своєю сутністю, це логіка спрощення. Умоглядна модель виступає, як якийсь еталон, пов'язаний з модельним уявленням про предмет зовнішнього та психологічного дослідження і виражений вже у формі робочої гіпотези на мові сформованої системи відповідних понять. В процесі моделювання професійного мислення юриста ми опрацювали такі етапи як: постановка задачі, створення моделі, вивчення моделі, створення систем моделей в залежності від інтерпретації результатів дослідження, застосування моделей в психологічних дослідженнях.

Процес моделювання ми розглядали, передусім, виходячи із принципу системності, згідно з яким будь-які психічні явища слід розглядати з позицій закономірності системного цілого і взаємодії складових його частин. Разом з тим ми спиралися на такі загальнометодологічні принципи як: діалектична багатосторонність опису об'єкта, єдність кількісних і якісних аспектів в описі об'єкта, єдність формалізованого і змістовного підходу, єдність теорії і практики. Основні принципи розглянемо нижче відповідно до визначень В. Г. Афанасьєва:

1. Органічна цілісність суб'єкта і об'єкта в процесі побудови моделі. Цей інтегральний принцип включає в себе ряд взаємопов'язаних моментів:

комплексність, інтегративність, міждисциплінарність системно-модельних прийомів.

2. Єдність структурності та ієрархічності моделей. Однією з фундаментальних рис психологічних моделей є наявність у них складної структури, яка так чи інакше повинна бути відображена в процесі моделювання. Досліджувану систему (або елемент системи) можна представити у вигляді певної структури з підсистем. При пошуку обґрунтованості того чи іншого розбиття слід враховувати нерівнозначність різних зв'язків між підсистемами і зберігати лише найбільше залежні одне від одного підсистеми та елементи.

3. Багатомодельність опису досліджуваних процесів і явищ. При збільшенні інформаційної ємкості моделі (а саме це відбувається при збільшенні числа врахованих параметрів) її ефективність (тобто можливість досить коректно і повно вирішити ті чи інші завдання) зростає не прямо пропорційно кількості врахованої інформації, а за екстремальним законом, тобто до певної межі, за якими ефективність даної моделі зменшується і необхідно переходити до іншої моделі.

4. Єдність формалізованого і неформалізованого опису. В рамках системного аналізу психологічних процесів і явищ очевидним є факт, що формалізований і змістовний опис досліджуваного об'єкта повинні доповнювати один одного [5].

Загальними принципами математичного моделювання згідно В. І. Міхееву, що виходять із загальних принципів системного аналізу, є:

1. Принцип достатності інформації, яка використається.

2. Принцип інваріантності інформації.

3. Принцип наступності.

4. Принцип ефективної реалізованості [6].

Змістовною основою для побудови математичної моделі об'єкта є його концептуальна модель. Під концептуальною моделлю об'єкта за О. В. Мангушевим розуміється сукупність якісних залежностей критеріїв

оптимальності та різних обмежень від факторів, істотних для відображення функціонування об'єкта. Концептуальна модель відображає такі основні моменти: умови функціонування об'єкта, зумовлені характером взаємодії між об'єктом і його оточенням, між елементами об'єкта [3].

При формулюванні концептуальної моделі системи інформаційної безпеки об'єкта виникають наступні проблеми (завдання): складання спрощеного і в той же час адекватної поставленої мети опису досліджуваної ситуації - сценарію функціонування об'єкта; формулювання і уточнення формулювання цілей, що стоять перед об'єктом при його функціонуванні; формалізація цілей в критерії оптимальності; формалізація зовнішніх і внутрішніх обмежень; вибір параметрів, що описують об'єкт і його оточення, які повинні бути враховані в дослідженні і відповідно включені в модель безпеки; класифікація параметрів і виділення з них в першу чергу керованих змінних [163]. Основна вимога до параметрів – вимірюваність.

Одним із основних завдань нашого дослідження було створення принципів побудови моделей інформаційної безпеки соціальних систем - підприємтсв. Основою для цього служили результати експертної оцінки, як одного з найбільше розвинених підходів для дослідження компетентності.

Ми вважаємо, що усереднені оцінки експертів не є показовими, тому що вони повинні бути співвіднесені зі структурою моделі та еталоном в обраному виді діяльності. В цілому, в уявленні експертів параметри оцінки є пов'язаними між собою через певні закономірності, якими визначається вплив на ефективність безпеко-забезпечуваної діяльності.

Рефлексивність – орієнтація на зовнішні аспекти. Рефлексивність включає в себе такі характеристики, як відтворюваність мислення (здатність індивіда розуміти власний хід мислення, його послідовність, логічність), здатність самостійно оцінювати результати свого мислення. Орієнтація на зовнішні аспекти по відношенню до самого процесу мислення, навпаки, полягає в прагненні до варіанту мислення, який є правильним з точки зору зовнішнього авторитету (прецендентність, доктринальність, нормативність).

Аналітичність – інтегративність мислення. Аналітичність полягає в тенденції до виділення приватного (дедуктивність), типовим прикладом може бути формалізм як високий рівень вимогливості до логічної строгості, правильності, стрункості юридичної думки. Інтегративність не зводиться тільки до індуктивності мислення, але також проявляється в здатності розглядати проблему з кількох різних позицій, розпізнавати факт в цілому за наявності мінімальної кількості його суттєвих ознак, а найбільшою мірою – в синтетичності.

Інструментальність – динаміка. Характеристики, що віднесені до категорії інструментальності, це перш за все «види мислення», а також понятійність (здатність оперувати юридичними і професійними поняттями), логіко-формальний характер мислення, (вміння моделювати ситуації, знаходити схожі до них за змістом та сенсом прецеденти, пояснювати їх, використовуючи логіку права). До динамічних ми віднесли такі характеристики, як високий рівень навченості, пізнавальна активність, інертність і/або швидкість мислення.

Організація – змістовність. Значення цих категорій є достатньо зрозумілим виходячи з самої назви, тому пояснимо лише те, що організація, зокрема, проявляється як систематизація, в процесі якої досліджувані об'єкти організовуються в певну систему на основі визначеного принципу. Змістовність, навпаки – в широті і глибині мислення, в характеристиках, що вказують на обсяг перероблюваної інформації.

Факторні навантаження таких параметрів, як гнучкість (здатність до адаптації і розвитку власних інтелектуальних схем при роботі з новою інформацією), дедуктивні (тяжіння до строгого в логічному сенсі аналізу, міркувань, мають адекватний формалізований апарат пізнання) і синтетичність (об'єднання розділених аналізом з виявленням при цьому істотних зв'язків) явно перевищують решту і переважно визначають зміст фактора.

Моделювання систем безпеки та експертні оцінки є одними із найбільше адекватними методами концептуалізації професійного мислення субєктів інформаційної безпеки. Тому основною метою нашої роботи є дослідження та

викреслення принпів створення моделей інфомаційної безпеки; наша ціль - створення єдиного універсальнго алгорітму побудови таких моделей для соціальної системи будь-якої фоми складності. Перш за все, побудова моделі повинна спиратися на вид і форму самої сціальної системи, а також на цілі та інтереси, які стоять перед соціальною системою (організацєю), які рухають і стимулюють вперед її дяльність.

Види моделей та моделювання різняться в науці залежно від класу закономірностей, яким підпорядковані модельовані об'єкти, а також від способів реалізації цього методу. У цій підставі виділяють: предметне або матеріально-реалізоване моделювання, яке полягає у створенні матеріальних моделей або підборі речових аналогів. Для деяких з цих моделей характерно схожість зовнішніх форм, а в ряді випадків і інших характеристик, притаманних оригіналу; логіко-математичне моделювання, яке полягає в описі засобами логіки і математики різноманітних відносин між предметами і явищами матеріального світу. Математичні моделі при необхідності досліджуються за допомогою комп'ютерів та інших технічних пристроїв, що дозволяють відтворювати структуру, динаміку процесів і явищ, характер зв'язку між елементами досліджуваних об'єктів і інші приховані властивості. Даний вид моделювання, як раз найбільше підходить для створення моделей систем інформаційної безпеки та інших дій по її забезпеченню. Саме такий вид моделювання ми і будемо досліджувати та розвивати.

Уявне моделювання - найменш розроблена область знання, її дослідження породжує дискусії, а пропоновані пояснення треба розглядати поки як гіпотези. Одна з таких гіпотез полягає в тому, що образні та логічні уявлення людини про навколишній світ можна трактувати як уявні моделі. Зовні вони можуть бути виражені у вигляді символів, знаків, схем, малюнків, конструкцій, засобами логіки і математики, і тоді уявне моделювання тісно пов'язується з іншими його видами.

Уявні (чи ідеальні) моделі поділяються на дві групи:

а) побудовані з чуттєво-наочних елементів (кулі, пружини, потоки рідини, силові лінії тощо), є зразками реальних явищ і доступних безпосередньому чуттєвому сприйняттю. Наочність цих моделей часто виражається у вигляді малюнків, схем, креслень (обставина, істотне і при моделюванні криміналістичних об'єктів);

б) виражені за допомогою знаків і комп'ютерних програм, і тому, що не мають зовнішньої схожості з об'єктом оригіналом. Способами реалізації уявної моделі є: опис зовнішніх ознак можливих подій, а так само наслідків до яких ці події призвели, виражені в графічному, фотографічному і комп'ютерному моделюванні цих ознак.

Остання, складає предмет дослідження численних наук, зокрема кібернетики, та фізико-математичних наук. Відомі дослідження з розробки формальної математичної моделі схем поділу секрету з пороговою структурою доступу, заснованих на використання китайської теореми про залишки.

Досвід показує, що в роботі по забезпеченню інформаційної безпеки соціальної системи (організації) складаються специфічні прийоми моделювання та особливі різновиди моделей. Найбільш прийнятними тут є логіко-математичні та розумові моделі, так як їх створення і вивчення найбільш доцільно у випадках із створенням систем інформаційної безпеки та незаконним доступом до конфедиційної інформації.Ми відходимо від традиційних моделей, які випливають із різновидів діяльності соціальних систем (організацій), або із сфери їх інтересів. Наше завдання та мета - розроблення моделей інфоромаційної безпеки без привязки до галузей, сфер та видів діяльності соціальних систем і їх субєктів. Ми ставимо за мету розробку моделей інформаційної безпеки придатну для вживання будь-якою організацією, класифікацію яких ми проводимо за власною схемою.

Розгляд типів моделей, способів їх створення і застосування, пропонуємо проводити за наступною класифікацією, визначаючи, таким чином алгоритм побудови моделі інформаційної безпеки:

•**залежно від сфери їх застосування,** та категорії конфіденційності інформації, щодо якої створюється модель,

•**залежно від складності соціальної системи (організації),** відносно якої забезпечуюється інформаційна безпека,

•**залежно від переліку та складу суб'єктів-виконавців** забезпечення самої системи безпеки.

Класифікація моделей за сферами застосування:

А) Моделювання при виробництві службових розслідувань щодо порушень режимів інформаційної безпеки організаціїдля отримання доказової інформації, використовується для перевірки наявних та отримання нових доказів, дослідження версій в тих випадках, коли пряме, безпосереднє вивчення об'єктів неможливо або недоцільно (наприклад, коли інформація несла комерційну таємницю і наслідки її розголошення відразу неможливо виявити, обстановка на місці події повністю або частково змінена, речові докази втрачені або не встановлені, пряме дослідження слідів на місці події не можна здійснити через відсутність для цього належних умов і т. д.). Нерідко необхідно перевірити версію про механізм здійснення події правопорушення. І оскільки використовувати при постановці дослідів наявну конфіденційну інформацію неможливо, у зв'язку з тим, що інформація, поки не отримала розголосу, як і раніше повинна вважатися конфіденційною, співробітник, який проводить службове розслідування, прибігає до моделювання.

З урахуванням цього, об'єктами моделювання (тобто тим, що піддається моделюванню) найчастіше є: різні предмети, цілісність яких зруйнована повністю або частково в результаті дій правопорушника або випадкових факторів (знаряддя злочину, окремі будови або частини їх, інструменти, комп'ютерна техніка, магнітні носії, програмне забезпечення, інші предмети); обстановка на місці події, що зазнала зміни в силу різних причин; сліди ніг, рук, взуття, транспорту, знарядь злому, інструментів та інших матеріальних предметів; документи, зниклі і зазнали зміни під впливом зовнішніх впливів (природних і злочинних); первісний зовнішніх вигляд об'єкта правопорушення і

злочинного впливу; ситуації, під якими слід розуміти певне положення, взаємодію предметів і осіб у період, що передував правопорушенню, в момент його вчинення і після нього; явища, пов'язані з досліджуваною подією, наприклад горіння, руйнування будь-яких пристроїв і т. п. Як різновид уявного моделювання можна розглядати образні уявлення, особи ведучого службове розслідування, про місце події, пов'язані з логічними судженнями про зовнішній портрет правопорушника, речових доказах, про зв'язки між людьми, предметами, явищами, що стосуються об'єкта правопорушення, тобто конфіденційної інформації. Подібного роду уявні моделі іноді отримують вираження у вигляді схем, планів, малюнків, креслень, словесних описів.

Об'єктами логіко-математичного та кібернетичного моделювання в службовому розслідуванні можуть бути ознаки спірних ситуацій, факти, що утворюють склад правопорушення, і пов'язані з ним обставини, відносини між предметами носіями інформації і явищами, ознаки інших слідів. І головне, що повинно досліджуватись виключно завдяки логіко-математичному моделюванню – це наслідки пошкодження, крадіжки та знищення конфіденційної інформації, які можливо дослідити після наявного правопорушення, яке не можливо допускати. Тому наслідки можливих вчинків, які настають також не відразу, вивчають завдяки уявному моделюванню.

Засоби і прийоми моделювання при виробництві службових розслідувань різноманітні. Доцільно розрізняти:

1) прийоми моделювання, щоб забезпечити отримання інформації про зовнішні форми і ознаки об'єктів-оригіналів, безпосереднє вивчення яких неможливе або ускладнене з об'єктивних причин. До їх числа відносяться: виготовлення зразків слідів, виготовлення макетів, що імітують окремі ознаки предмета чі явища; підбір або виготовлення предметів аналогів для огляду, постановки дослідів, опитувань, пред'явлення для впізнання; уявне моделювання, яке отримує вираження у вигляді схем, малюнків окремих предметів; матеріальна реконструкція (відтворення) первісного стану предметів

і документів носіїв інформації; математичне моделювання в експертизі слідів, почерку;

2) прийоми моделювання, щоб забезпечити отримання інформації про яку-небудь ситуацію (первинному положенні предметів на місці події, положенні правопорушника і об'єкта посягання, послідовності дій правопорушників та ін.) Для цих цілей використовуються: реконструкція обстановки на місці події, реконструкція дій всіх можливих учасників події, що допомагає встановити, напрямок витоку або переміщення інформації, і вирішити інші питання; реконструкція обставин події, уявне моделювання у вигляді схем, планів, підбір предметів аналогів для постановки дослідів; математичне моделювання;

3) з позицій моделювання можна розглядати і такі технічні прийоми відображення, як фотографування, відео- та звукозапис мови, комп'ютерне та програмне моделювання.

Майже всім названим прийомам притаманна поліфункціональність. Так, виготовлення схематичних планів, фотографування, відеозйомка, звукозапис є традиційними засобами фіксації, детально розробленими криміналістикою з урахуванням завдань розслідування.

Фотознімки, відео-,звукозапис та комп’ютерне проргамування, як моделі цікаві тим, що відображають не тільки зовнішні ознаки об'єкта, а й процеси, що протікають у часі і недоступні безпосередньому сприйняттю людини. Сучасні технології дозволяють відтворити об'єкт у трьох вимірах і виробляти відповідні дослідження.

На відміну від інших матеріальних моделей, об'єкти – аналоги, створені завдяки комп’ютерній техніці, використовуються не замість оригіналу, а поряд з ним, вони не замінюють оригінал, а включаються разом з ним в процедуру. У цьому одна з характерних особливостей моделювання в службовому розслідуванні, що допускає різні варіанти використання моделей.

Необхідно зауважити, що жорстке розмежування способів моделювання неможливо: всі вони пов'язані між собою і взаємообумовлені. Досить сказати, що створення (вибір) і використання будь-якої матеріальної, математичної

моделі опосередковано мисленням. У свою чергу уявні моделі - уявлення перевіряються за допомогою інших видів моделювання.

Суб'єктами моделювання в розслідуванні можуть бути: співробітник служби безпеки, який веде розслідування, експерт, фахівець, запрошений для участі у виробництві службового розслідування, підозрюваний, свідок, потерпілий.

Б) При виробництві товарознавчих та інших експертиз,моделювання є методом експертного дослідження. В якості об'єктів моделювання виступають: окремі предмети носії інформації, явища, ситуації, пов'язані з досліджуваною подією, ознаки слідів, почерку та ін.

Застосування моделей залежить від виду інформації і цілей експертиз, конкретних методик їх проведення. Так, в якості моделей можуть використовуватися піддослідні співробітники, що імітують спосіб заволодіння інформацією та спосіб її передачі, не розкриваючи її справжнього змісту, якщо виникає необхідність перевірити реакцію співробітників на деякі події.

Зазначений підхід заснований на провокативній моделі взаємодії, заснований на продукування дезінформації. В класичній соціальній психології він відповідає моделі лабораторного експеримента.

Дезінформація - свідомо помилкова інформація, що надається противнику або діловому партнерові для більш ефективного ведення конфронтаційних дій, співпраці, перевірки на витік інформації і напрямок її витоку, виявлення потенційних клієнтів чорного ринку.

Також дезінформацією (дезінформуванням) називається сам процес маніпулювання інформацією: введення кого-небудь в оману шляхом надання неповної інформації або повної, але вже не потрібної інформації, спотворення контексту, спотворення частини інформації.

Відомі наступні види дезінформації:

- введення в оману конкретної особи чи групи осіб (в тому числі і цілої нації);
- маніпулювання (вчинками однієї людини або групи осіб);

•створення громадської думки щодо якоїсь проблеми або об'єкта.

Виділяють такі рівні маніпулювання:

•посилення існуючих у свідомості людей вигідних маніпулятору цінностей (ідей, установок ...);

•часткову зміну поглядів на ту чи іншу подію або обставини;

•кардинальна зміна життєвих установок.

Створення громадської думки - це формування в суспільстві певного ставлення до обраної проблеми.

В якості реконструкції ситуації можна розглядати і відомі органам безпеки «Операція під чужим прапором», «фальшивий прапор», «операція під чужим прапором», «фальшиві кольори» - таємні операції, здійснювані з метою переконати громадськість в тому, що ці операції проводяться іншими організаціями або державами.

Операції під фальшивим прапором проводяться під час війни, операцій проти повстанців, а також в інших випадках (наприклад ї при здійсненні стратегії напруженості). Перераховані дії стають конкретними моделями впливу.

У криміналістичій експертизі застосовується матеріальне моделювання, зустрічаються логіко-математичні та кібернетичні моделі, різні реконструкції, має місце використання предметів - аналогів у якості моделей, фотографування та інші прийоми.

Суб'єктами моделювання в експертній практиці є фахівці у певній галузі науки, техніки, виробництва, що виступають в якості експертів при проведенні службового розслідування, програмісти, IT- фахівці, лаборанти, що працюють під керівництвом експерта.

В) Моделювання в організаційно-управлінської діяльності, що забезпечує організацію процесу створення системи інформаційної безпеки підприємства, профілактики правопорушень і витоку інформації.

Об'єктами моделювання тут можуть бути:

•процес утворення та забезпечення зберігання конфіденційної інформації;

•процес обігу та використання конфіденційної інформації суб’єктами відносин;

•взаємодія керівництва та підлеглих співробітників підприємтсва під час робочого процесу;

•дії суб’єктів, що забезпечують інформаційну безпеку (керівники, охоронці, співробітники та ін.) під час виникнення нештатних ситуацій.

В якості прийомів моделювання використовуються уявні моделі про життєздатність системи безпеки підприємства, розмежування функцій співробітників залежно від ступеня доступу до інформації, і їх дії (буденні і при виникненні нештатних ситуацій). Створюються моделі характерних правопорушеннь, їх причини, механізми виконання, утворення слідів, напрямку службового розслідування. Моделювання за допомогою комп'ютера для вирішення організаційно - управлінських завдань з великим обсягом інформації, одночасна і швидка оцінка якої не під силу людині. За допомогою комп'ютера моделюється програма можливих наслідків, за заздалегідь розробленим алгоритмом.

Різновиди моделей організаційно-управліньської діяльності залежать від розміру самого підприємтсва, кількості рівнів доступу та обміну конфіденційною інформацією, наявності та кількості співробітників служби безпеки. Але єдиним залишається те, що при створенні моделей систем інформаційної безпеки, необхідно залучати та враховувати весь наявний персонал підприємтсва, лише так можливо врахувати всі можливі шляхи розвитку подій і наслідків. При чому кожен співробітник повинен бути визначеним суб’єктом інформаційної безпеки, знати та дотримуватись прийнятої (затвердженої) моделі поведінки та відносин.

Найбільш складним завданням на шляху вирішення цих проблем є кодування ознак, що характеризують складну, нештатну ситуацію, кримінально-правові, кримінально-процесуальні, цивільно-правові, цивільно-процесуальні, адміністративні та інші норми права. Дані моделі, на

підприємтсвах, закріплюються в мережевих планах, що забезпечують наочність планування та затверджуються наказами.

Г) Для створення позитивного іміджу підприємтсва, під час конкурентної боротьби із конфліктним супротивником, який може вести інформаційну боротьбу, направлену на приниження підприємтсва бажано створювати моделі, націлені на припинення конфликтних дій. Дані моделі повинні бути адекватні розміру загрози та можливим наслідкам та збиткам від інформаційної атаки конкурента.

Об'єктами моделювання в такому разі можуть бути:

- організація роботи підприємтсва;
- відносини між керівниками та підлеглими;
- зовнішній імідж підприємства та його керівників;
- позитивна думка співробітників підприємства та пересічних громадян стосовно керівництва та самого підприємства.

В якості прийомів моделювання використовують уявні та логіко-матеамтичні моделі, які приймуть керівники підприємства, що затверджують стратегію інформаційної політики підприємтсва. Які зможуть створити всі суб'єкти інформаційної безпеки підприємтсва. А також які найбільш коректно відповідатимуть інтересам, цілям та завданням підприємства [7].

Залежно від складності соціальної системи (організації):

Розробляючи системи безпеки соціальних систем організацій, відносно яких забезпечуюється інформаційна безпека, слід враховувати наступне:

а) психологічну модель управління, що діє в організації,

б) складність структури соціальної системи.

А) Психологічні різновиди управління організаціями можуть поділятись на авторитарні та колегіальні. При цьому важливу складову відіграють відносини в середині соціальної системи (організації).

Відомі числені дослідження з приводу того як можуть складаютися відносини між субєктами забезпечення безпеки та членами організації, між самими членами організації, між керівництвом та всіма іншими, тощо.

Встановлено, що якщо соціальна система була створена штучно (завод, підприємство) то правила відносин між членами та субєктами є навязаними зверху, а значить, що в середині системи обовязково виникнуть звязки неофіційного характеру.

В цьому контексті ми розуміємо наступне. У зв’язку з примусовістю (задана с самого початку) певної ієрархії в організації, не маючи права впливу та вибору організаційної структури, співробітники так чи інакше, безпосередньо, або опосередковано укаладтимуть «власну» ієрархію. Чим більше організаційна структура буде асоціюватися у свідомості співробітників зі станами домінування, небезпеки, незадовілняння потреб, тим у більшій кількості випадків актуалізуватиметься неформальна організаційна структура, що популяризуватиме альтернативні організаційні цінності та схеми взаємодії. В цьому контексті доречно згадати про психоаналітичний термін «відреагування в зовні». Пояснемо чому саме цей процес є важливим у розумінні нами феноменології інформаційної безпеки.

Наскільки відомо, вперше поняття "відреагування" з'явилося в психоаналітичній літературі при описі дій пацієнтів поза офісом, коли їх поведінка реалізовувала почуття, спрямовані на аналітика, але які пацієнт боявся відчувати або допустити до усвідомлення, особливо в присутності психоаналітика. Пізніше цей термін стали використовувати в основному для опису поведінки, обумовленої несвідомою потребою справитися з тривогою, асоційованої з внутрішньо забороненими почуттями та бажаннями, а також з нав'язливими страхами, фантазіями і спогадами.

У зв’язку з цим, екстраполюючи зміст данного процесу на контекст організаційної структури, зазначимо, що відігрування в зовнє відповідає механізму витіку інформації, пошуку середовища, яке б відповідало ідеальним уявленням. Часто такий підхід сприяє становленню опозиції, просуванню ідей зовнішніх агентів, тощо.

Одночасно з неформальними лідерами в соціальних системах є офіційне керівництво, яке діє згідно із статутами та інструкціями. В залежності від того,

скільки керівників в соціальній системі та яким чином риймаються рішення, їх поділяють на авторитарні (керує одна особа) та колегіальні (дві та бальше осіб).

Виходячі із вищевказаного, вважаємо, що неможливо створювати модель інформаційної безпеки соціальної системи не враховуючі їснуючі офіційні та неофіційні міжособистісні зв'язки.

Б) Складність структури соціальної системи відіграє важливу роль під час створення моделей забезпечення безпеки, тому що від цього залежить комунікація між підрозділами, швидкість обміну інформацією та якість відтворення керівних команд, разом із їх виконанням. Соціальні системи слід розглядати, в залежності від різновидів їх інтересів та видів діяльності, на горизонтальні та вертикальні.

Горизонтальні мають у себе на меті досягнення інтересів та діяльності в одній галузі, наприклад торгівлі або бідівництві. Таки соціальні системи (організації) мають у складі однорідних субєктів та членів системи, які займаються приблизно однаковий рівень інтересів. Склад таких систем утворюється в залежності від обємів діяльності, але він однорідний. Наприклад будівельна компанія має на мету розширення своїх потужностей, і при збільшенні, підвищує кількіть працівників однорідних профессій та обслуговуючого чи адміністративного персоналу. Виходячи с цього необхідно створювати модель безпеки націлену на захисть однорідних функцій, від одних і тих же можливих посиганнь. При збільшенні потужностей соціальної системи, може збільшуватись кількість субєктів забезпечення безпеки по горизонталі системи. Але це не впливатиме на саму модель та процедури відтворення діяльності системи безпеки.

Вертикальні соціальні системи, створюють ті горизонтальні системи, які досягли певного розвитку та почалисвоє розширення в інші, не притаманні їм галузі, або створюють вертикальну ланку від видобування сировини до розповсюдження своєї продукції. Прикладом такої соціальної системи (організації) може бути нафто-видобувна компанія, яка перейшла від самого видобування нафти до її переробки, до виготовлення певного переліку пального

та смазочних матеріалів, придбавши для цього виробничі потужності, розширивши їх, а потім створила свою мережу по оптовому та роздрібному збуту своєї продукції.

В даному випадку ми маємо більш складну модель забезпечення інформаційної безпеки, яка розповсюджується на горизонтальні складові соціальної системи, які мають однорідні інтереси (однорідний набор дій по забезпеченню безпеки), а також вертикальні складові, що складаються із різних рівнів горизонтальних моделей для кожного різновиду інтересів окремо. Вертикальна модель інфоомаційної безпеки забезпечуює комунікацію між горизонтальними рівнями, між собою та керівництвом, вона виконує функцію склеювання та утримування соціальної системи від розгалуження та руйнування. В такому разі збільшення інтересів соціальної системи не завжди призводить до збільшення субєктів забезпечення безпеки, тому що у вертикальних моделях інфомаційної безпеки, одні і тіж субєкти можуть виконувати свої функції на різних горизонтальних рівнях. В таких моделях важливо приділяти увагу якості комунікацій між горизонтальними рівнями та керівництвом. При цьому, різні горизонтальні рівні повинні мати різні ступені допусків до конфіденційної інформації, різний (свій) перелік охороньованої інфоромації.

За аналогією, можемо стверджувати, що держава – є найскладнішою соціальною системою із вертикальною структурою, тому наш підхід до побудови моделей інформаційної безпеки придатний для створення державних (національних) систем інформаційної безпеки.

Ми вважаємо, що інформація - основний продукт інформаційного суспільства і особливий об'єкт правового регулювання в сферах публічного і приватного права. Вона відіграє вирішальну роль в сучасному суспільстві, всі області життєдіяльності суспільства опосередковуються інформаційними засобами і здійснюються в інформаційному просторі. Саме тому інформаційна безпека стала одним з головних факторів, що визначають національну,

регіональну і міжнародну безпеку, а її забезпечення - одним з головних пріоритетів держави [7].

Залежно від переліку та складу суб'єктів-виконавців:

Забезпечення самої інформаційної безпеки здійснюється субєктами (людьми) соціальної системи, які відрізняються між собою і мають власні інтереси та проблеми. На нашу думку до процесу участі в забезпеченні інформаційної безпеки повинні бути причетні всі субєкти, і ті, що безпосередньо займаються її здійсненням, і ті, до основних обов'язків яких це не входить.Взагалі то, такими субєктами можуть бути звичайні співробітники, якщо на підприємстві немає окремої підрозділу служби безпеки. В такому разі функції по забезпеченню інформаційної безпеки покладаються в повному обсязі на весь персонал.

Слід також зазначити, що не можна ототожнювати поняття «захист інформації» та «інформаційна безпека». Інформаційна безпека це не тільки захист інформації, але і організаційні, адміністративно-правові та інші заходи, спрямовані на забезпечення сталого, стабільного розвитку окремої соціальної системи і суспільства в цілому. У зв'язку з цим дуже важливо розуміти, що інформаційна безпека є соціальним, а не чисто технічним явищем. Поняття «інформаційна безпека», «безпека інформації», «захист інформації» взаємодоповнюють один одного. При цьому кожна наступна категорія є складовою частиною попередньої.

В своїх моделях ми розробляємо такі механізми, які призведуть до мінімізації впливу людського фактору на здійснення інформаційної безпеки.

Розглянемо детальніше. Поняття «людський фактор» в нашій країні традиційно пов'язується з проблемою аварійності, оскільки саме людина, як правило, є тою самою «слабкою ланкою» в технологічному ланцюгу сучасного виробництва.

В численних науково-психолоігчних дослідженнях є спроби розробити концептуальний підхід для системного розгляду впливу людського фактора на статичні та динамічні процеси в організаціях та інституціях. Відомо про зв'язки

темпераменту з регуляторно-динамічними, а також продуктивно-смисловими ознаками ініціативності особистості. Визначено специфіку зв'язків ініціативності і різних параметрів активності людини.Розкрито міжрівневий зв'язок між динамічними, інструментальними, особистісними і соціально-психологічними властивостями суб'єкта: зв'язок властивостей темпераменту і акцентуацій характеру, спрямованості міжособистісних відносин в колективах, зв'язок акцентуації характеру і міжособистісних відносин.

Ми маємо на меті концептуалізувати наступне. Проблема людського фактора полягає у відсутності достатніх знань про природні закони поведінки людини, про причинно-наслідкові зв'язки впливу на людину різних чинників. Проблема починається з відсутності визначення поняття «людський фактор», в якої складності і часом неможливості на сьогоднішній день формалізації складових людського фактора, у відсутності методології кількісної оцінки і врахування впливу людського фактора на безпеку соціальної системи, держави.

В якості методологічного орієнтиру може виступити математичний апарат теорії нечітких множин (НМ), теорії ймовірностей і математичної статистики, сучасні спеціальні діагностичні методики для визначення типологічних ознак, що характеризують структуру міжособистісних відносин членів групи, а також використовувалися результати тестування діяльності членів колективу.

Одне із основних завданнь створених моделей інформаційої безпеки, враховуючи субєктні особливості, полягає в тому, що мінімізувати вплив особистості на роботу моделей інформаційної безапеки, унеможливити ненавмисне втручання в діяльність соціальної системи, виключивши фактори помилок та неналежний рівень кваліфікації субєктів безпеки.

Зазначене може бути досягнуто з урахуванням наступних принципів моделювання інформаційної безпеки, як:

1. Адекватність актуального стану інформаційної моделі цілям прогресивного розвитку суспільства;

2. Використання адміністративно-правових інформаційних моделей, як одного з головних засобів суспільно-державного управління;

3. Відповідність моделей інформаційної безпеки життєво важливим інтересам держави, суспільства і особистості, національним інтересам країни в цілому;

4. Спрямованість на недопущення зовнішніх і внутрішніх інформаційних загроз;

5. Реальна можливість вростання інформаційної політики України в міжнародному інформаційному простірі;

6. Відкритість, гласність і доступність інформаційної політики для розуміння її різними соціальними категоріями населення;

7. Демократичний порядок формування інформаційної політики, її підконтрольність представницьким органам влади і суспільства в цілому;

8. Забезпечення збереження інформаційних ресурсів, їх адміністративний і організаційний захист, як одного з головних елементів стратегічного розвитку держави і суспільства;

9. Здатність молелей інформаційної безпеки створювати всі необхідні умови для впровадження національних і регіональних інформаційних систем і технологій [8].

В закінченні сдід зазначити, що всі моделі повинні бути економічно адекватними тим затратам та цілям, задля яких вони створюються. Тому логічно, що вони повинні, перш за все, бути націлені на попередження небажаних нападів. А це може бути досягнуто, якщо змодельована дія стосуватиметься стриманню протиправних дій. Процес стримання повинен стосувались інтересів потенційних агресорів та зловмисників. Тобто модель дій повинна показувати опонентам, що протиправні дії відносно підприємтсва створять для нападника відповідні збитки їх головним інтересам. Створені моделі краще всього відповідатимуть своїм основним завданням, якщо будуть пов’язані із так званими непрямими діями, що не вказують прямо на кінцеву свою ціль і мету, а вводять в оману агресора, надихають на віддану працю співробітника та стимулюють виконувати свої обов’язки сумлінно всіх суб’єктів інформаційної безпеки підприємтсва.

Список використаних джерел:

1. *Карпенко З. Аксіопсихологічний поворот у психології особистості: досвід методологічної реконструкції / З. Карпенко // Психологія особистості. - 2010. - No 1. - С. 180- 185.*
2. *Максименко С. Д. Генетико-моделюючий метод дослідження особистості / С. Д. Максименко // Науковий вісник Миколаївського національного університету імені В. О. Сухомлинського. Серія : Психологічні науки. - 2014. - Вип. 2.13. - С. 8-16.*
3. *Шмелев А. Г. Психометрические основы психодіагностики / А. Г. Шмелев // Общая психодиагностика / под ред. А. А. Бодалева, В. В. Столина. – М : МГУ, 1987. – С. 53 - 112.*
4. *Афанасьев В. Г. Системность и общество / В. Г. Афанасьев. – М. : Наука, 1980 – 250 с.*
5. *Мангушев А. В. Диагностика профессионального мышления на этапе совершенствования мастерства специалиста : на примере специалиста экологического профиля : дис. ... канд. психол. наук : спец. 19.00.13 / Александр Валерьевич Мангушев : МГУ. – М. : РГБ, 2003. – 158 с.;*
6. *Луньов В.Є. Становлення та розвиток професійного мислення особистості у системі органів внутрішніх справ України : Монографія / В.Є. Луньов - Макіївка: МЕГІ, Донецьк: Донбасс, 2013 – 350 с.*
7. *Михеев В. И. Моделирование и методы теории измерений в педагогике / В. И. Михеев. – М. : Высшая школа, 1987 – 230 с.*
8. *Мельник С. И. Теоретико-информационный подход к анализу измерительных данных и оценке их неопределенности / С. И. Мельник // Системи обробки інформації. - 2009. - Вип. 5. - С. 43-46.*
9. *Prisniakova, L.M., Prisniakov, V.F. Mathematical model of the interpersonal conflict on the spacecraft during long mission (2005) International Astronautical Federation - 56th International Astronautical Congress 2005, 1, pp. 219-227.*

4.5. SECURITY OF ELECTRONIC BANKING IN POLAND

ANNA KORZENIOWSKA *PhD*
WOJCIECH MISTEREK *PhD*
Maria Curie-Skłodowska University in Lublin
Faculty of Economics, Department of Banking

Introduction. The development of electronic banking, its rate and diversity are followed by emerging new forms of risk. It is connected both with new technologies, attacks by criminals (hackers) as well as carelessness of bank customers. The most common crimes related to security of customers of electronic banking include an illegal way to acquire customers' identifiers and passwords - and to use them later, phishing, fraudulent e-mails, card theft and its unauthorized use, etc. Such tools as spyware, Trojan horses or malware[19] are also employed.

There is an increasing activity of cybercriminals. As estimated, in 2014 in Poland on average some 280 thousand computers were infected for every 24 hours. Yet, by the CERT survey the most alarming trend was the increase in attacks on Internet banking users. Moreover, in Poland Trojans attacking electronic banking are ranked fairly high among active Trojan horses. [20]

Hence, there is a number of activities which aim at reducing risk of using electronic banking by bank customers. These activities are run by regulators, Banking Supervision and banks themselves. Measures taken to increase security of electronic banking include legal regulations setting out rights and obligations of banks, their customers who use this kind of banking and institutions providing technologies, standards worked out by international institutions which facilitate co-operation between banking institutions and indicate the direction for the development of

[19] Yazdanifard R., Wan Fadzilah WanYusoff, Alawa Clement Behora¸ Abu Bakar Sade, *Electronic Banking Fraud; The Need To Enhance Security And Customer Trust In Online Banking,* International Journal in Advances in Information Sciences and Service Sciences, 2011; 3(10.61):505-509.
[20] CERT Polska Raport 2014, NASK, Warszawa 2015.

electronic banking; e.g. SWIFT standards, banks' operations connected with risk management as well as educational activities addressed to bank customers.

1. Principles for electronic banking

Among principles concerning risk management are, inter alia 'Risk Management Principles for Electronic Banking' published by the Bank for International Settlements in July 2003[21]. They are relatively general and divided into three groups:

"Group A. Board and Management Oversight (Principles 1 to 3):

1. Effective management oversight of e-banking activities.
2. Establishment of a comprehensive security control process.
3. Comprehensive due diligence and management oversight process for outsourcing relationships and other third-party dependencies.

Group. B. Security Controls (Principles 4 to 10):

4. Authentication of e-banking customers.
5. Non-repudiation and accountability for e-banking transactions.
6. Appropriate measures to ensure segregation of duties.
7. Proper authorisation controls within e-banking systems, databases and applications.
8. Data integrity of e-banking transactions, records, and information.
9. Establishment of clear audit trails for e-banking transactions.
10. Confidentiality of key bank information.

Group C. Legal and Reputational Risk Management (Principles 11 to 14):

11. Appropriate disclosures for e-banking services.
12. Privacy of customer information.
13. Capacity, business continuity and contingency planning to ensure availability of e-banking systems and services.
14. Incident response planning"

In Poland, of special importance are the recommendations and information systems made available to banks by the Polish Bank Association (ZBP) – a chamber of commerce established by banks operating in Poland. One of the educational

[21] *Risk Management Principles for Electronic Banking*, BCBS, July 2003, pp. 7-8.

activities carried out by ZBP is giving recommendations with regard to the use of electronic banking and payment cards. They are the following:

1. ZBP recommendations related to electronic banking

i. Remember, no bank ever sends to its customers inquires on passwords, confidential information, or any requests for their updating.

ii. Check on your bank's website what safeguards are used in the bank's Internet service.

iii. A computer or a mobile phone connected to the Internet must have antivirus software installed and kept updated.

iv. Make online payments only using 'secure' computers'.

v. Contact your Internet provider to make sure they use secure distribution channels for their services.

vi. Have only legal software installed on your computer.

vii. Periodic computer scanning is recommended, particularly before entering the bank's website and performing any transactions.

viii. Keep the operating system updated, as well as applications, essential for its functioning, e.g. web browsers.

ix. Do not open emails or attachments of unknown origin.

x. Avoid websites encouraging to watch attractive content or special offers.

xi. On logging into the transaction system do not go away from your computer and after the session log out and close the Web browser.

xii. If, while logging in you get unusual messages or request for your personal data, or additional field with the question about a password for authorization, report the problem immediately to your bank.

xiii. Do not enter the website of your bank through the links given by incoming e-mails. (Phishing). Neither is it recommended that you use bookmarks (Firefox) or 'favourite contacts' (Internet Explorer), as there are malicious object able to modify addresses which are saved there.

xiv. Never use search engines to find the login page of your bank. The links found there may redirect you to fake websites or pages with viruses.

xv. Before you log in, check if the connection with the bank is secure. The website address of your bank should start with the abbreviation: "https://", not "http://".

xvi. Check the authenticity of the certificate.

xvii. Never share your user's identification or access password with any third party.

xviii. Do not write down passwords to encode your log in data anywhere and remember to change them regularly. An ideal solution is to reset a password once a month, but as long as such a change is not enforced automatically by the system, do it at least every two months by using a combination of lower and upper case letters and numbers.

xix. Check the date of the last correct and incorrect jogging into the system.

xx. Use telephone hot lines made available by your bank.

xxi. Monitor on regular basis the portal 'Secure Bank'(Bezpieczny Bank) on the ZBPwebsite – www.zbp.pl [22]

ZBP recommendations related to the use of payments cards were published separately:

i. While performing a transaction do not leave the card out of sight. Once the transaction is completed, take it back immediately.

ii. Special care must be taken while transferring the card number. Do not disclose the card number to anyone who calls you, also when the caller informs about problems with the computer and asks for verification of the information. It is not a practice for companies to call and ask for the number of the credit card. If you call first, do not disclose the card number either, when you are not sure that the other person may be trusted.

iii. Never respond to electronic mail which requires giving information on the card. Never answer those emails which invite you to visit a website to verify the data, including those referred to the card.

iv. Never give any information about the card on websites which are not secure.

[22] https://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa

v. Sign the card immediately on its receipt.

vi. Destroy before any possible disposal credit cards applications which may be mailed to you.

vii. Never write down your PIN on the card or keep it together with the card (against the theft of your wallet or purse).

viii. Never leave the card or transaction receipts unattended.

ix. Protect your card number and other confidential codes which enable to perform transactions (e.g. PIN number, CVV 2 number, CVC2 number by registering the image of the card, e.g. by using a mobile phone with a photo camera, video camera, or any other way, so that unauthorized persons could not take possession of it

x. Compile a list of card numbers as well as addresses and phone numbers of the banks whose cards you hold; keep it in a safe place. The list should be updated every time you get a new card.

xi. You need to carry with you only these cards which are necessary. You shouldn't carry with you cards which are rarely used.

xii. Treat card transactions with similar caution as any other transaction made on your account. Check the transactions performed immediately upon receipt of account statements for debit cards and a list of transactions for other cards. Keeping the receipts of payments allows for immediate verification.

xiii. In the event of any discrepancies a complaint in writing should be placed with the bank which issued the card.

xiv. Always destroy incorrect receipts, collect receipts of those transactions which were not executed.

xv. Before throwing away, destroy all the documents including the full number of the card.

xvi. Never sign receipts in blanco. In the case of transactions executed with an imprinter (it refers only to embossed cards) always cross out a line in an empty field in the form so that fraudulent additional payments are not possible.

xvii. Tracing paper is used very rarely, but having used it in card transactions, destroy it.

xviii. In restaurants, on receiving a terminal printout with a field for a tip, write down the amount of a tip or cross out this field with a horizontal line.

xix. Never write down your PIN in a place accessible to the public.

xx. It is advisable to carry your cards not in the wallet, but preferably in a separate closed compartment or attaché case.

xxi. Never give your card to anyone.

xxii. If you are moving, do not forget to inform immediately the bank, which issued the cards, of any change of address.

xxiii. Do not take with you the card if its use is unlikely as you risk losing it (e.g. while shopping on the open street markets or other places where you might be exposed to pickpocketing). If you have been in a situation which encourages theft, check if you have your cards (e.g. while travelling).[23]

Apart from recommendations ZBP takes also concrete preventive actions. To report a theft or loss of payment cards in a more effective way a special info line was activated. The customer does not need to remember the bank's telephone number; he may apply for stopping of his cards in different banks in one place. Of special importance is also the system 'Classified Documents'. It is a data base of information on identifiers lost by the bank's customers: identity cards, passports, driving licensees, etc. Since 2008, i.e. the date when the system came into operation, 61 200 attempts of swindling credits amounted to 3,3bn PLZ [24] were defeated. To enter the data into the system, it is enough for the customer to report losing his documents in any bank operating on the territory of Poland and co-operating with the system. The database also collects data on stolen documents from system of the Police.

Out of the existing laws in Poland which govern the safety in the functioning of electronic banking, the greatest impact has the Payment Service Act.[25] It implements into Polish legislation the provisions of Directive 2007/64/WE of the European

[23] https://zbp.pl/dla-konsumentow/bezpieczny-bank/karty-bankowe
[24] infoDOK, Raport o dokumentach, 24 Edition, Q4 2015 , p. 4
[25] *The Payment Service Act of 19 August 2011,* Journal of Laws of 2011 No. 199 Item 1175.

Parliament and of the Council of 13 November 2007 r.[26] It sets out rights and obligations of persons using electronic banking, including electronic access to bank accounts and payment cards . It stipulates all the circumstances under which the liability for lost funds is assumed by the bank and when by the customer.

To illustrate better the state of electronic banking in Poland, it is necessary to quote some characteristic numbers (Table 4.2).

Table 4.2

Statistics describing the state of electronic banking in Poland

State on 30 September 2015	Specification
30 323 788	Number of individual customers with a written contract for using Internet banking
14 642 409	Number of active individual customers
5	The average number of transfers of an active individual customer per month (qty)
5 784	The average value of settlements of an active individual customer per month (PLN)
2 176 835	Number of SMEs customers with a written contract for using Internet banking
1 287 470	Number of active SMEs customers
18	The average number of transfers of active individual customer of SME per month (qty)
66 989	The average value of settlements of an active SME customer per month (PLN)
408,75	Number of operation in ELIXIR* system (mld pices)
1 066,76	Value of operation in ELIXIR system (bln PLN)
28 617 797	Number of issued debit cards
5 862 753	Number of issued credit cards
27 600 000	Number of paypass and pay wave cards (aprox.)
869,90	Number of transactions with payment cards (mld)
134,11	Value of transactions with payment cards (bln PLN)
21 647	Number of ATM (aprox.)

* ELIXIR – clearing system in Poland run by Krajowa Izba Rozliczeniowa

Source: NetB@nk, RAPORT Bankowość Internetowa i Płatności Bezgotówkowe, III q 2015, ZBP, p. 3.

[26] Directive 2007/64/WE of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market-PSD amending Directives 97/7/WE, 2002/65/WE, 2005/60/WE and 2006/48/WE and repealing Directive 97/5/WE (Text with EEA relevance)

2. Perception of risk from using electronic banking by students of the City of Lublin

2.1. Description of research method and research sample

The subject of the analysis presented in this paper is the research on functioning the students of Lublin City conducted in 2015 by The Student Society of Financiers of Faculty of Economics at UMCS under the authority and supervision of the research Staff of Department of Banking. The research was carried with the usage of two research techniques CAWI (Computer Assisted Web Interviewing) and direct questionnaire surveys. The questionnaire was addressed to 852 respondents, 562 of who were women (65,96%), and 290- men (34,04%). Among the surveyed dominant were students of studies free of charge who accounted for 68,58% of the research sample. While analyzing the mode of courses one can note that the main group consisted of students of full-time education (72,96%). In the group of part-time students there were only 4 persons (0,51%), while extramural students accounted for 26,53% of the research sample. Among the surveyed there were 48 persons (5,63%) who took up studies at a few faculties, and the majority of who are students of two courses. The data analysis form Figure 1 demonstrates that the biggest group of the respondents was made up of the students of Maria Curie-Skłodowska University in Lublin (33,22%).A large proportion was accounted for by the students of Lublin Technological University, Lublin Medical University, Lublin University of Life Sciences, Lublin Catholic University of John Paul II and Lublin University of Economics and Innovation; their students accounted for between 9% and 15% of the research sample. Other smaller university units had a much smaller share in the sample. The focus of the research on this age group resulted , among others ,from the fact that the penetration ratio in this group is the highest and it amounts to 95%, while for the whole population it is 77%.

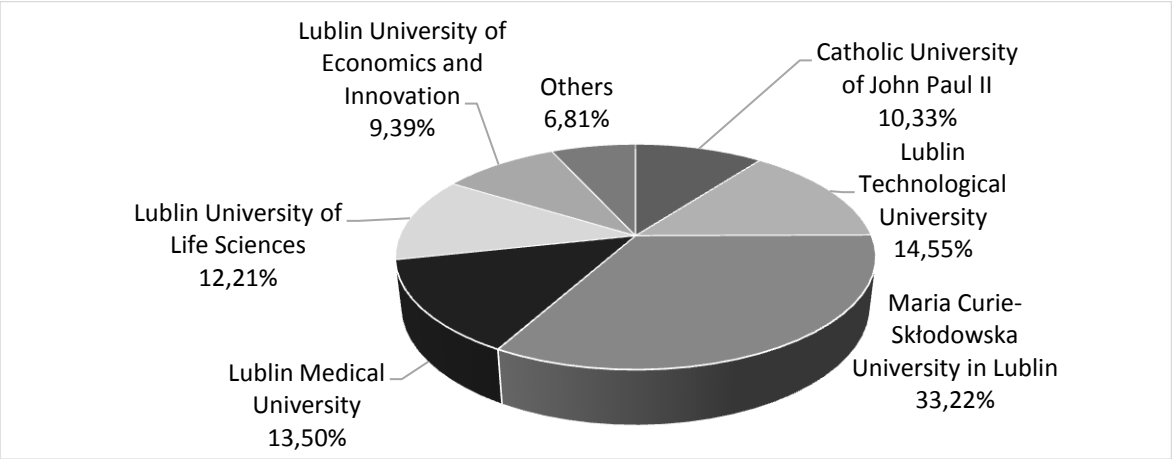


Figure 4.7. Respondent structure by university

Source: Authors on the basis of questionnaire surveys.

The research sample appropriately takes into account also the structure of students depending on the place of residence. Among the respondents the majority were residents of villages (46,48%) and the biggest urban centre, i.e. Lublin (19,37%). A much lower share in the sample were residents of small and medium-size towns who in total accounted for less than 35%.

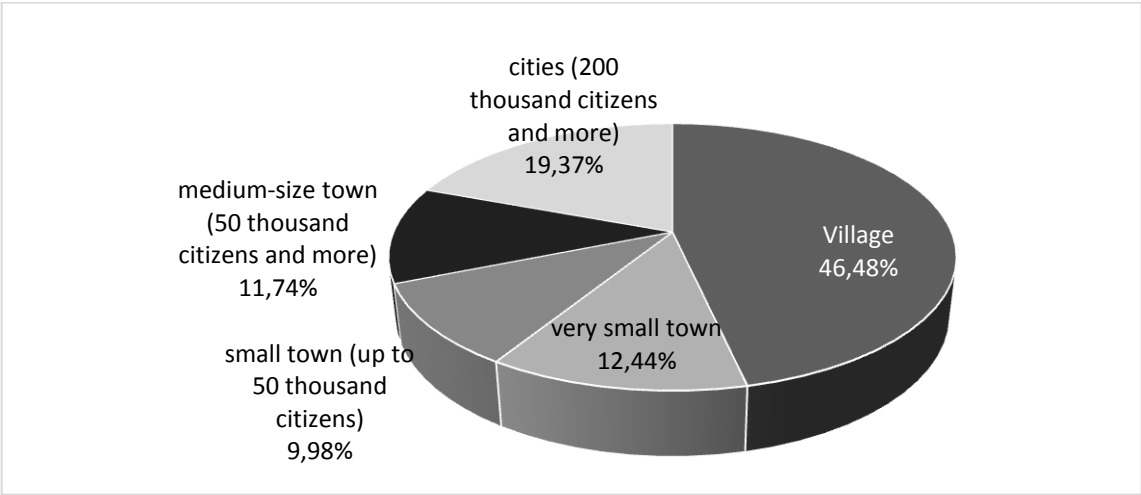


Figure 4.8. The structure of respondents by the place of residence

Source: Authors on the basis of questionnaire surveys.

While concluding one may notice that that the structure of the research sample fully reflects the structure of students of Lublin universities- both in terms of factors

related to the choice of study, faculty or modes of courses, as well as in terms of demographic factors.

The above research will be confronted with the findings of the research run in 2012 as a part of the scientific project 'Using bank services by households in Lublin Voievodeship'. Within the framework of the project questionnaire survey was carried out ,one element of which was to assess the use of electronic banking. The research was addressed to 365 respondents residing in Lublin Voievodeship. The surveys were completed by 231 women who represented 63,29% of the surveyed group and 134 men who made 36,71%. The majority of the respondents were persons under 20(3,84%) and above 60 (nearly 5,48%). The remaining groups aged 31to 39, 40 to 49 and 50 to 59 had a similar share in the sample at the level of 16-18%. As for education, prevailing were respondents with university degrees (nearly 36%) and secondary school education (approx.35%). Only 10 persons declared basic education and 7 persons were holding the academic title. Four persons taking part in the research did not give any answer to the question about their education.

2.2. Universality of holding a bank account and using electronic banking

Table 4.3

Universality of holding a bank account and the period of its use

Bank product	I do not use	1year	2-3 years	4-5 years	6-7 years	More than 7 years
Savings and settlement account (ROR)	46,9%	11,3%	20,1%	15,0%	3,2%	3,6%
Savings account	74,6%	7,9%	8,3%	7,5%	0,5%	1,2%

Source: Authors on the basis of questionnaire surveys.

While analyzing the data from Table 2 one may observe a rather low universality of holding a bank account by students. Slightly over 50% of the respondents hold savings and settlement accounts, while savings accounts – only15,4% of the surveyed persons. Moreover, over a half of the students with

savings accounts declared also the possession of savings and settlement accounts. For comparison, the research run among the adult residents of Lublin Voievodeship revealed that over 72% of the respondents are bank account holders.

In comparison, the research done among adult residents of Lublin Voievodeship showed that over 72% of the respondents are bank accounts holders. Yet, it is worth pointing out that the percentage of bank account holders increases along with a mode of study; for non-stationary students the percentage is close to 67%, while for stationary students – 49%. This can be explained by the fact that among non-stationary students there often appear older persons who have already had some employment and families which encourage them to take use of banking services earlier. Similar differences can be seen according to the place of residence. A little more than 45% of the students living in small towns or villages have bank accounts and for the surveyed who live in large or medium cities this percentage is 60%.

The examined students ,as for their age, are characterized by a fairly long time experience in using the discussed banking services. Some more than 21% of account holders have been using them for less than a year and the majority are persons who have been using banking services for 2-3 years (37,86%) and 4-5 years (28,21%). It should be emphasized that more than 12% are persons who have been holding bank accounts for over 6 years. It proves a high penetration ratio of young persons as well as effective bank policy meant to promote their services to the youngest customers.

Examining the data from Figure 3 one can observe that the surveyed students who are bank account holders are characterized by the high universality of using Internet banking , as only 3% do not use this access channel. It is a much lower percentage than that of the research run for households of Lublin Voivodeship, where as many as 26% of the respondents admitted their reluctance of using Internet access channel to the bank account. This result comes from the fact that for young people it is more commonplace to function in the online environment. Besides they are not in the habit of using traditional distribution channels (e.g. bank branch) which are still popular especially with elderly people.

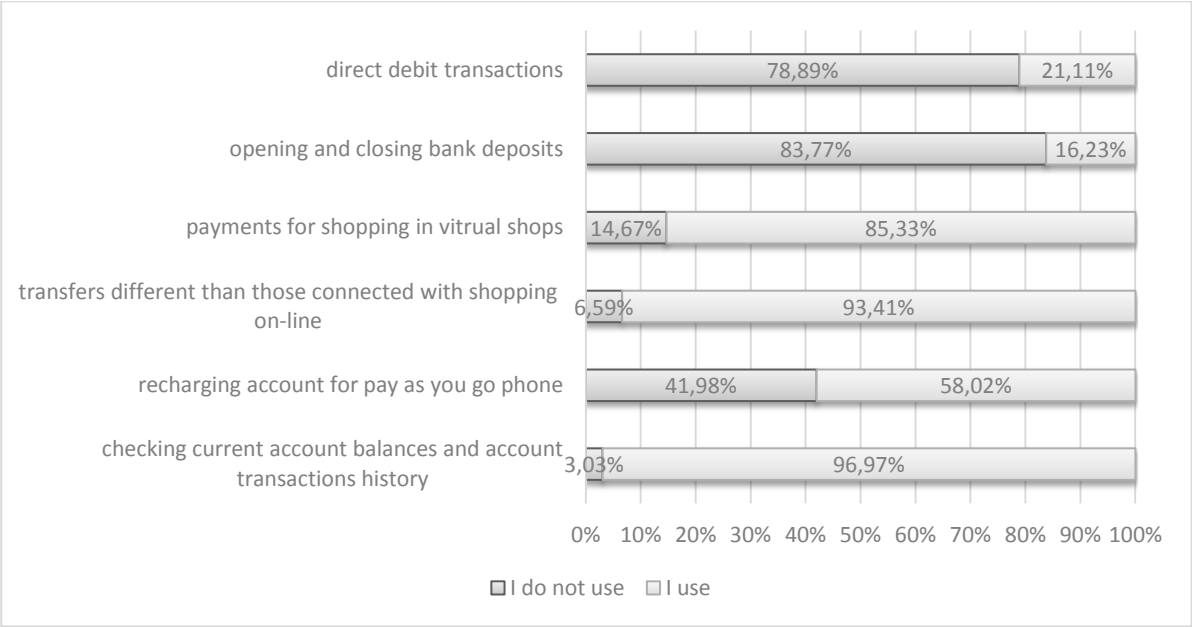


Figure. 4.8. Universality of using Internet banking for performing particular banking operations

Source: Authors on the basis of questionnaire surveys.

All the students using Internet banking declared using it to check current account balances or account transaction history. A slightly lower percentage of persons indicated the use of Internet banking for the execution of transfers different than those connected with shopping online (93,41%) and settling payments connected with shopping in virtual shops (85,33%). Consequently, it becomes evident that the change of the model of customer service and shifting the burden of payment settling to modern channels of data transmission have met with high acceptance of young bank customers. It is also confirmed by the high universality of using payment systems (53,49%) dedicated to settle virtual shopping (e.g.. Pay U, pay via Allegro, or transfers 24). These systems are not only to speed up payment execution for shopping but also to ensure a higher level of security both for customers and the virtual shop.

Internet banking was the least frequently used by the respondents for direct debit transactions (21,11%) and for opening or closing bank deposits (16,23%).This is due to a limited number of regular payments realized by the students and the low universality of savings term deposits.

In recent years banks have been developing data transmission systems more often through applications installed on mobile phones This channel of performing services is to a greater extent adjusted to meet expectations of a younger generation. However, as shown by the research, the universality of its use is far lower than the one of the Internet services. Mobile banking is used by less than 21% of the surveyed students, the majority of who (92,86%) use it to check the balance of the account or the transaction history. A considerable lower number of students , than in the case of internet banking, use it to execute transfers other than those connected with shopping online (67,01%) or settling payments connected with shopping in virtual shops (55,25%). Other operations which use this access are performed occasionally. Still the low universality of using mobile banking, even by the youngest bank customers, is likely to be the consequence of inappropriate preparation of banking applications installed on mobile phones as well as the users' opinions on a higher risk of performing transactions through this access channel.

Another channel of electronic banking verified in the research were payment cards. The possession of this instrument was acknowledged by 80,46% of the surveyed students which is nearly twice as many as in the research done among adult residents of Lublin Voievodeship (40,65%). It proves their greater acceptance of a basic instrument of electronic money and that they are less accustomed to cash. In both types of research the respondents admitted holding debit cards but among the students this group constituted 71,49% of the sample, whereas among the residents of the voievodeship - merely36,16%. Noticeably, smaller is the disparity with credit cards which is due to the specificity of this instrument and its direct link with credit less frequently taken by young people. It refers practically exclusively to older students of non-stationary or evening studies. What is worth noting is the fact that some students have credit cards linked with the credit taken out by their parents, which considerably raises the universality of the use of this instrument. With other cards (virtual and prepaid), their universality is at a very low level and does not exceed several percent.

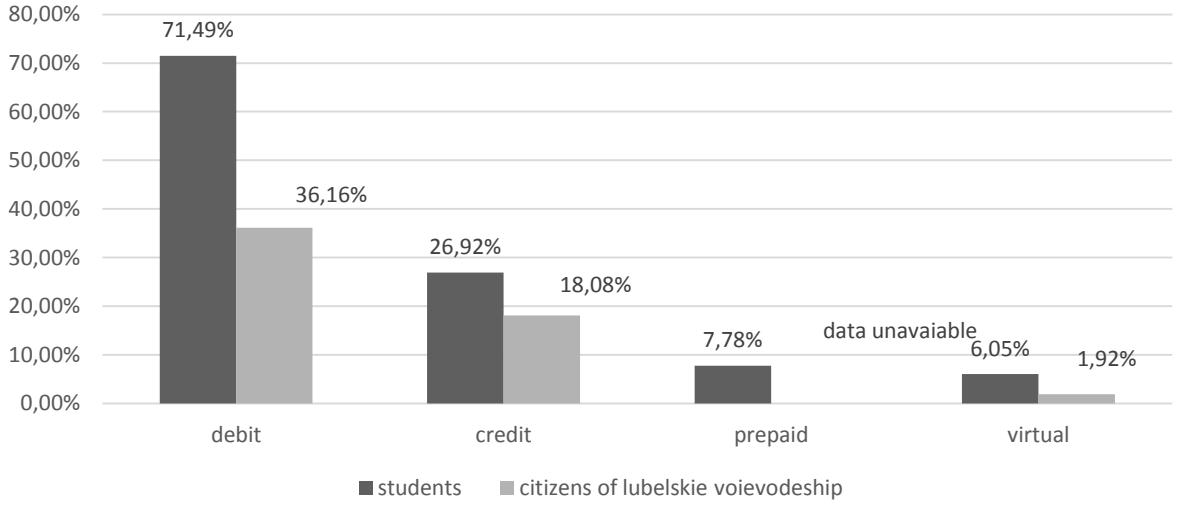


Figure 4.9. Universality of using payment cards by the students of Lublin City and the adult residents of Lublin Voievodeship

Source: Authors on the basis of questionnaire surveys.

2.3 Evaluation of security of particular banking instruments by the students of Lublin City

The analysis of data presented in Figure 5 shows explicitly that the students see the risk arising from using particular channels of electronic banking. Security for all the analyzed instruments was assessed lower (3,91) compared with a traditional form of contact with the bank via its branch (5,28). It is confirmed by the median set for the first case with the grade 4 and for traditional banking at the level 6. It proves that the research group shows great awareness of threats arising from using modern access channels and of still insufficient security on the part of both the legal system and the banks.

Additionally, one can observe that the evaluation of security was affected by experience in the usage of particular instruments. It means that instrument less poplar in the investigated group were assessed as more hazardous, though it is not always reflected in the real market of a given channel of performing banking services. It is confirmed by far higher evaluations of such channels as direct online access though the bank's website, payments by payment card in a non-virtual shop, ATM or a cash deposit machine, which were 4,36 up to 4,56 and the median was set with 5. For comparison, transactional instruments using short text messages (SMS) or online

payments dedicated to serve online shops whose security is even bigger than pointed in the students' evaluations, were assessed as much riskier and were placed at the level 3,49 - 4,12. It seems that it was the effect of limited knowledge as well as the lack of the usage of this tool in practice.

Interestingly enough, the security of systems connected with the use of smartphones, which is now most actively promoted by banks, are assessed relatively very low. It refers both to the dedicated applications for serving the bank account (3,46) as well as systems of contactless payments NFC - near-field communication - (3,28). It points at a high level of imperfections of these systems in terms of safeguards and the lack of the bank's proper information policy on their security.

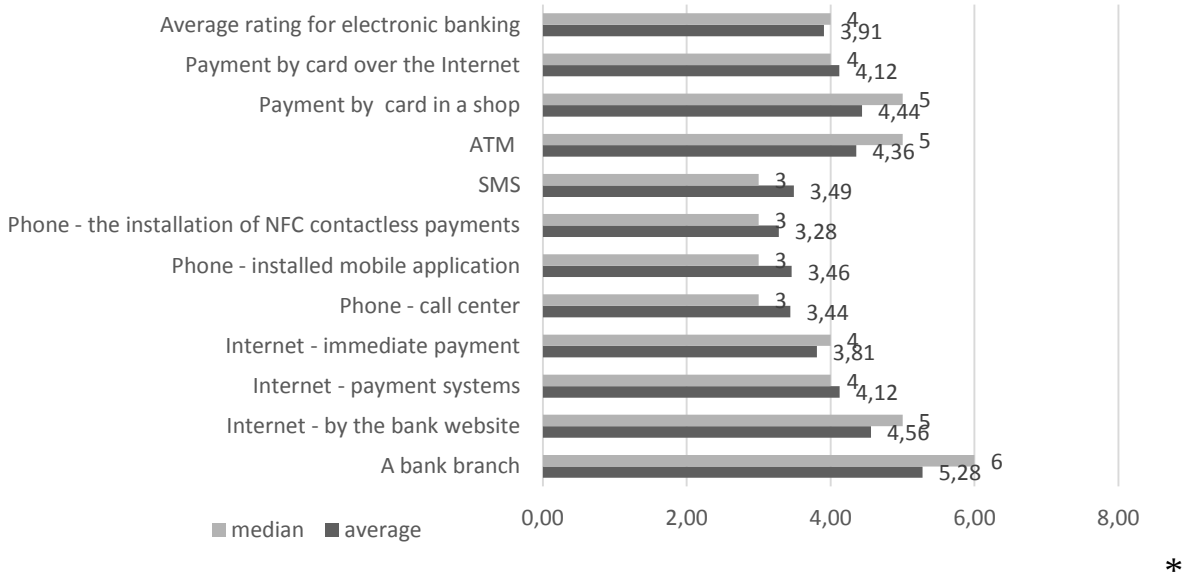


Figure. 4.10. Evaluation of using particular instruments of electronic banking compared to evaluation of traditional channel of performing banking services *

*scale: 1- no secure use, 6 – channel completely safe

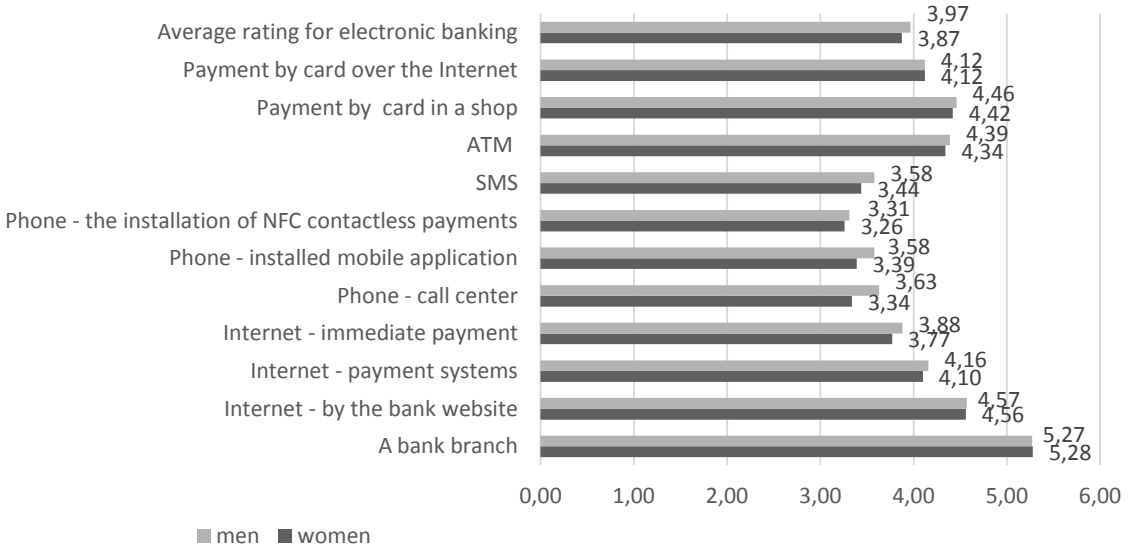
Source: Authors on the basis of questionnaire surveys.

The median set for both cases as 3 confirms it. Finally, it is interesting to note that the students' evaluation of the risk coming from using payment cards in the Internet appears to be fairly appropriate. It is one of most often used instruments to steal in electronic banking. It seems, however, that their assessment does not translate directly into exercising caution by the questioned students. It is exemplified by a very

low universality of using prepaid cards which allows to a greater extent minimize risk and reduce the amount of potential loss.

2.3.1 Gender of respondents

The data from Figure 6 show a small impact of gender on the assessment of risk of using electronic banking. It is worth noting, that the average evaluation by women is definitely lower, which may result from their smaller acceptance of risk and greater awareness of it. What is more, the differences become evident mainly for applications installed on smartphones and systems of Internet payments , both connected with virtual shopping and instant shopping. In both cases lower assessment of security may be viewed as the result of a lower universality of using. As shown by the research analysis only16,6% of women and as many as 24,1% of men use mobile banking when systems increasing security and speed of virtual shopping are used by 47,2%of men and 42,6% of women. Thus, the earlier conclusion may only be confirmed again, namely, that we assess higher the risk for instruments which we do not know or use.



*

Figure 4.11. Evaluation of security while using particular instruments of electronic banking against a traditional channel of performing banking services made by men and women *

*scale: 1- no secure use, 6 – channel completely safe

Source: Authors on the basis of questionnaire surveys.

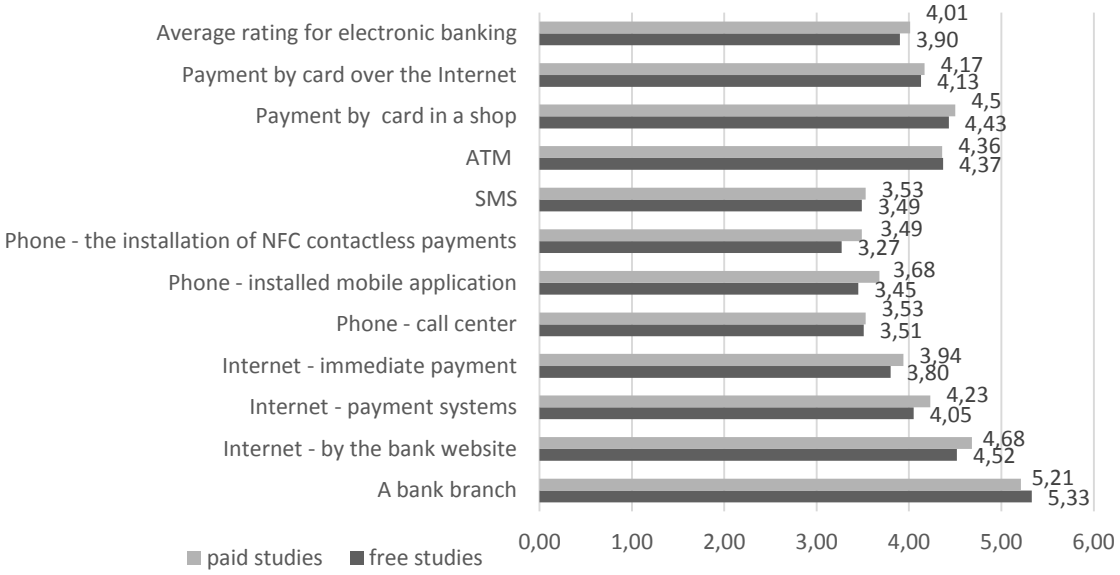
2.3.2Students of studies free of charge and studies paid

Noticeably bigger disparities in the risk evaluation of particular instruments are evident with the comparison made by students of studies free of charge and those of paid studies. The research results show the students of the first group perceive the risk of electronic banking as higher. It is clear both in the average evaluation of security of electronic access channels, which for the first group was3,90 4,01, as well as when compared with the evaluation of the traditional access channel while visiting a bank branch. This time it was assessed higher (5,33) by the students of studies free of charge than by the students of paid studies(5,21). One may rightly assume that, similar to the analysis of gender, the decisive factor for these differences is the universality of using of particular access channels, which is higher for the respondents paying for their studies. Moreover, the evaluation of higher security of electronic banking in this group may be impacted by longer experience in using banking services. As the research shows the average age of students incurring costs of education is 1,5 year higher, which undoubtedly translates into more experience of using banking services. A share of employed persons also is influential on experience as they use banking system in their professional practice. Surprising was the fact, that, stark differences in the evaluation appear in the case of mobile banking and contactless payment systems installed on smartphones. These technical solutions are more willingly used by students who do not incur any educational costs. In this case it might be rightly assumed that negative experience is likely to be this factor which decreases the safety assessment.

2.3.1Influence of employment on the perception of security in electronic banking

The previous analyses showed that the factors which influence the perception of risk in using particular channels of electronic banking are knowledge and experience in their use. In this context, it is reasonable to compare the employed and unemployed students to verify if work experience also translates into the perception of risk. The data in Figure 8 confirm this thesis as the evaluation of security of all the instruments of electronic banking is significantly lower among the unemployed respondents than the employed ones – both in full- time and temporary jobs. The

persons with full time employment assess the security much higher than the persons with temporary jobs.



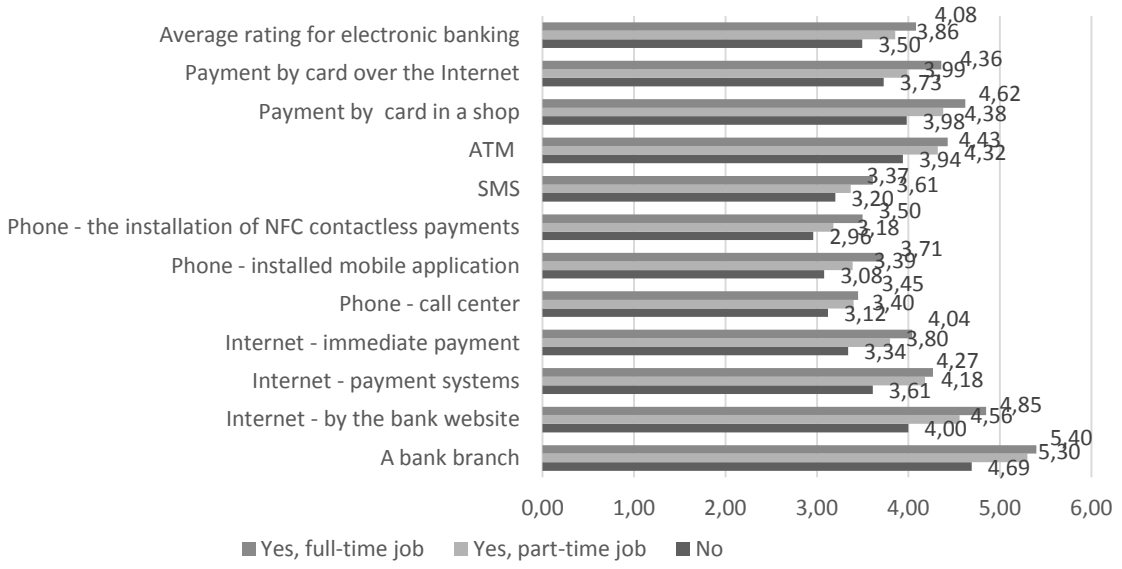
*

Figure 4.12. Evaluation of security in using particular instruments of electronic banking against evaluation of traditional channel of providing banking services made by students of free and paid studies *

*scale: 1- no secure use , 6 – channel completely safe

Source: Authors on the basis of questionnaire surveys.

Therefore, it can be concluded that work experience, which at least partly requires the usage of banking services decreases risk thanks to the process of 'taming it'. And thus, the more often the respondent uses a given service, the more he is prone to minimize perceiving risk. However, it is worth noting that this phenomenon refers not only to electronic access channels, but also to the direct contact in the bank branch. The students who work, especially full-time, and who have more experience of co-operation with the bank, assess its security much higher which results from their positive experiences.



*

Figure 4.13. Evaluation of security of using particular instruments of electronic banking against the evaluation of the traditional channel of providing banking service made by the students of free and paid studies*

*scale: 1- no secure use, 6 – channel completely safe

Source: authors on the basis of questionnaire survey

2.4 Opinion of adult residents of Lublin Voievodeship on the risk connected with using electronic banking

The research conducted among the students of Lublin City showed clearly a far lower level of safety in the use of electronic banking compared with the traditional access channel. Similar conclusions may be drawn on the basis of the research which was conducted in 2012 among the adult residents of Lublin Voievodeship. At that time the respondents were to compare various aspects of risk for these both channels.

As the data from Table 3 show the biggest risk in the respondents' opinions are the dangers arising from technical problems of the banking system, including potential leaks in the system and attacks of persons from outside. A higher level of this was indicated by over 42% of the respondents, i.e. three times more than in the case of traditional banking.

Table 4.4

Households' opinions on risk connected with using electronic banking

Risks	Yes, and it is higher compared with traditional banking	Yes, and it is lower compared with traditional banking	Does not exist	Difficult to say	Lack of data
In electronic banking there is risk coming from bank frauds	36,16%	13,97%	10,68 %	31,78%	7,40%
In electronic banking there is risk coming from the bank employee's error	12,05%	21,92%	27,40 %	31,23%	7,40%
In electronic banking there is risk coming from the bank customer's error	34,79%	17,26%	9,59%	29,04%	9,32%
In electronic banking there is risk coming from technical problems of the banking system	42,19%	13,42%	7,12%	29,04%	8,22%

Source: Authors on the basis of questionnaire surveys.

According to the surveyed, higher risk of electronic banking is caused by bank frauds and bank customers' errors. In both cases around 35% of the respondents stated that this risk is higher in electronic banking than in traditional one; an opposite view was held by several percent of the persons questioned. While the opinions on the latter one seem to be justified, as the essence of using modern ITC solutions is higher automation of the process and shifting the burden of the service onto the customer himself - hence the higher risk in this area, bank frauds , however, refer to the same extent to these both areas of banking. It would be good to remember, however, that a substantial part of risk in electronic banking, and Internet in particular, result from the failure to maintain an appropriate level of security by customers themselves. However, the information on potential frauds with the usage of electronic channels is perceived by the surveyed as mistakes on the part of banks and not customers themselves. Thus, there is such a high evaluation of this risk related to electronic banking.

For comparison, respondents noticed that the human factor brings along a far greater risk in the case of traditional banking. It seems, however, that in the

respondents' opinion the meaning of this risk is the least. It may be proved by a fairly big group of persons who can't perceive this risk in the both distribution channels (27,4%).

Summary. Despite a wide range of actions taken by supervisory institutions and banks, customers still perceive electronic banking as less secure than using banking products directly in bank branches. First of all, they are afraid to make mistakes by themselves when using banking product as well as of frauds and embezzlement committed by the third parties. Yet, contrary to these fears a number of customers using electronic banking who are interested in new forms of this banking, as e.g. mobile banking, is still growing.

References:

1. *Directive 2007/64/WE of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market-PSD amending Directives 97/7/WE, 2002/65/WE, 2005/60/WE and 2006/48/WE and repealing Directive 97/5/WE (Text with EEA relevance)*
2. *CERT Polska Raport 2014, NASK, Warszawa 2015.*
3. *https://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa*
4. *https://zbp.pl/dla-konsumentow/bezpieczny-bank/karty-bankowe*
5. *infoDOK, Raport o dokumentach, 24 Edition, Q4 2015*
6. *NetB@nk, RAPORT Bankowość Internetowa i Płatności Bezgotówkowe, Q3 2015, ZBP, Risk Management Principles for Electronic Banking, BCBS, July 2003,*
7. *The Payment Service Act of 19 August 2011, Journal of Laws of 2011 No. 199 Item 1175.*
8. *Yazdanifard R., Wan Fadzilah WanYusoff, Alawa Clement Behora¸ Abu Bakar Sade, Electronic Banking Fraud; The Need To Enhance Security And Customer Trust In Online Banking, International Journal in Advances in Information Sciences and Service Sciences, 2011; 3(10.61):505-509.*

РОЗДІЛ 5
КОНТРОЛЬНО-АНАЛІТИЧНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ РИЗИКАМИ КОРПОРАТИВНОГО ШАХРАЙСТВА В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

ГНИЛИЦКАЯ ЛАРИСА ВЛАДИМИРОВНА, *д.е.н., професор*
професор кафедри бухгалтерського обліку
ДВНЗ «Київський національний економічний університет ім. В.Гетьмана»

5.1. АНТИКОРУПЦІЙНИЙ АУДИТ ЯК ІНСТРУМЕНТ ПРОТИДІЇ КОРУПЦІЇ ТА ХАБАРНИЦТВУ У ДІЯЛЬНОСТІ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

Протягом усього часу існування незалежності України проблема корупції та шахрайства не сходить із сторінок засобів масової інформації, постійно констатується негативний факт активного розповсюдження цих явищ та посиленого їх проникнення в усі сфери життєдіяльності держави та суспільства.

В сучасних економіко-політичних умовах корупція та шахрайство набули ще більших масштабів, що істотно перешкоджає економічному зростанню України та реально загрожує її національній безпеці. Для подолання економічних злочинів у сфері бізнес-відносин підприємств України запроваджено Закон про антикорупційну діяльність, який спрямований на визначення загальних засад запобігання корупції та шахрайства у діяльності юридичних осіб.

Однак, більшість антикорупційних заходів органів влади носить формальний характер і зводиться до ухвалення документів політичного характеру. Між тим, за результатами Всесвітнього огляду економічних злочинів, частка корпоративного шахрайства з кожним роком зростає. При цьому до галузей економіки, підприємства яких найбільше страждають від недобросовісних економічних стосунків відносять фінансові послуги (50% респондентів зіштовхнулися з випадками злочинів), енергетичну та гірничодобувну промисловість (43% респондентів), галузь зв'язку (40% респондентів).

Структура економічних злочинів також досить різноманітна. Зокрема, у 2015 році 73% опитаних підприємств заявили, що постраждали від незаконного привласнення активів, 60% респондентів регулярно у своїй діяльності зіштовхуються з наслідками конфлікту інтересів, а 30% опитаних зазначають, що найсуттєвіші економічні злочини спричинили маніпуляції з фінансовою звітністю. При цьому 85% жертв шахрайства не повертають свої кошти [1].

Слід зазначити, що на відміну від попередніх років, які відзначалися незначною питомою вагою економічних злочинів скоєних співробітниками

підприємства, у 2015 році частка злочинів, спричинених діями персоналу склала вже 72%. При цьому простежується тенденція, що розміри шахрайства, скоєні співробітниками спричиняють більший збиток, ніж зловживання зовнішніх суб'єктів.

Зазвичай корупція та шахрайство у діяльності суб'єктів господарювання включає такі основні елементи:

- фальсифікація фінансових показників - внесення завідомо неправдивих даних у фінансову звітність. Метою є обман акціонерів, податкових органів чи власників підприємства (шахрайство топ-менеджменту);
- незаконне привласнення активів: крадіжки, розтрати; оплата невідпрацьованого часу (шахрайство середньої ланки управління та безпосередніх виконавців);
- корупція різного роду – комерційний підкуп, що потребує не облікованого готівкового грошового потоку так званої «чорної каси» (проявляється в системі «відкатів»);
- конфлікти інтересів – тобто наявність у особи приватного інтересу у сфері, в якій вона виконує свої службові чи представницькі повноваження, що може вплинути на об'єктивність чи неупередженість прийняття нею рішень, або на вчинення чи не вчинення дій під час виконання зазначених повноважень (використання інформації, що становить комерційну таємницю з метою особистої вигоди, створення фірм-посередників, що належать друзям, чи членам родини тощо).

До основних напрямів корпоративного шахрайства та корупції відносять:

- продаж товарів та послуг зі знижкою з метою отримання «відкатів»;
- придбання активів та послуг за завищеними цінами і не завжди найкращої якості;
- крадіжки на складах, чи в касі підприємства (через не оприбутковані, чи задвоєні документи);
- формування не облікованих готівкових коштів з метою подальшого їх використання при наданні хабарів: оплата консультаційних послуг не існуючого характеру; виплата матеріальної допомоги окремим категоріям персоналу; реалізація продукції з формуванням безнадійної дебіторської заборгованості;

- постановка на баланс підприємства з відповідним обслуговуванням основних засобів, якими користуються посадовці, що отримали їх в якості хабара тощо.

Існування значного спектру корпоративного шахрайства та корупції породжує необхідність запровадження системи дієвих заходів для упередження випадків економічних злочинів.

За даними світових обстежень, проведених аудиторською компанією «Ернст енд Янг», у 2015 році одним із основних антикорупційних заходів респонденти назвали антикорупційний аудит (контроль) (72% опитаних). За своєю популярністю він поступився лише виконанню принципів корпоративної етики (90% опитаних), обійшовши при цьому такі традиційні заходи протидії корупції як наявність «гарячої лінії» для анонімного повідомлення випадків корупції та шахрайства (32%) та юридична перевірка контрагентів (10%).

Відтак, з метою використання антикорупційного аудиту в системі внутрішнього контролю підприємств України виникає необхідність теоретичного обґрунтування його сутності та визначення методичного інструментарію.

Під *антикорупційним аудитом* слід розуміти систему перевірок здійснюваних антикорупційним аудитором, спрямованих на ідентифікацію ризиків корпоративного шахрайства та оцінювання виконання антикорупційних заходів на підприємстві.

Для більш глибокого розуміння сутності антикорупційного аудиту у таблиці 5.1 надано основні відмінності у функціях та методології проведення антикорупційного аудиту та аудиту господарської діяльності.

Контрольні заходи в системі антикорупційного аудиту можуть носити як профілактичний (упереджу вальний), так і реактивний характер.

Зокрема профілактичний контроль передбачає встановлення персональної відповідальності за активи та рішення, які підконтрольні певній посадовій особі. Для цього у трудових угодах та посадових інструкціях слід виокремити пункти, які визначають каральні заходи при встановленні ознак шахрайства у поведінці співробітника.

Таблиця 5.1

Відмінності аудиту господарської діяльності та антикорупційного аудиту

Ознака	Аудит господарської діяльності	Антикорупційний аудит
Регулярність	Проводиться з чітко встановленою регулярністю	Здійснюється за наявності достатніх доказів виявлення випадків шахрайства, а тому не носить регулярного характеру
Мета	Здійснення експертизи щодо достовірності фінансових даних наданих у відповідних документах	Встановлення наявності фактів корпоративного шахрайства, винуватця та ступеня його вини
Характер процесу здійснення аудиту	Процес проведення аудиту не носить ворожого характеру	Процес виявлення випадків шахрайства є за своєю сутністю ворожим, бо спрямований на встановлення винуватця та ступеня його вини
Методологія	В основу покладено традиційні методи дослідження достовірності даних бухгалтерського обліку	Окрім перевірки фінансових даних використовують способи фактичної перевірки активів, психологічні методи, спеціальні способи забезпечення економічної безпеки тощо

Реактивний контроль передбачає запровадження системи контрольних процедур, що дозволить виявляти корупційні ризики та факти господарської діяльності пов’язані з умисним порушенням співробітниками своїх обов’язків.

Враховуючи склад економічних злочинів, спричинених корупцією та шахрайством, антикорупційний аудитор виконує наступні завдання:

- проводить непланові (тематичні) перевірки фінансової документації та фактичної наявності активів;
- здійснює моніторинг ризиків корупції та шахрайства;
- приймає участь у проведенні службових розслідувань виявлених випадків корупції та шахрайства (опитування свідків, пошук документальних доказів);
- здійснює оцінювання достовірності фінансової звітності з метою раннього діагностування маніпуляцій з фінансовими показниками.

Для виконання зазначених завдань антикорупційний аудитор використовує способи контролю, аналізу, менеджменту персоналу та безпекознавства, серед яких:

- обмеження доступу до інформації;
- непланова інвентаризація активів;
- непланова (вибіркова документальна перевірка діяльності окремих посадових осіб чи менеджерів середньої ланки управління);
- контроль за здійсненням окремих операцій (перевірка «нетрадиційних» угод, перевірка динаміки простроченої дебіторської заборгованості, перевірка змін у стані розрахунків з окремими дебіторами; перевірка фактичного стану складського господарства тощо);
- запровадження «гарячої лінії»;
- атестація персоналу (перевірка на лояльність);
- інформування колективу підприємства про факти виявлення корупційних схем та випадків шахрайства тощо.

Узагальнення способів та прийомів антикорупційного аудиту при виконанні завдань щодо протидії корупції та хабарництву в діяльності суб’єктів господарювання надано в таблиці 5.2.

Не викликав сумнівів, що запровадження антикорупційного аудиту на підприємствах України стане дієвим механізмом протидії корпоративному шахрайству та уможливить зниження негативних тенденцій, спричинених діяльністю персоналу підприємства, пов’язаною з використанням наданих йому службових повноважень з метою одержання неправомірної вигоди.

Однак, як показали дослідження сучасної практики господарювання більшості вітчизняних підприємств, серйозною проблемою, що стоїть перед їх керівництвом при запровадженні антикорупційного аудиту є: відсутність організаційно-правового забезпечення такої діяльності на законодавчому рівні, безсистемний характер наявних методичних розробок щодо використання технологій аудиту, аналізу та безпекознавства у антикорупційній діяльності, а

також не адаптованість системи підготовки подібних фахівців у вітчизняних учбових закладах до вимог ринку відповідних послуг.

Таблиця 5.2

Способи антикорупційного аудиту при виконанні завдань протидії корупції та хабарництву

Завдання антикорупційного аудитора	Способи антикорупційного аудиту
Здійснення непланових (тематичних) перевірок фінансової документації та фактичної наявності активів	1) обмеження доступу до інформації; 2) непланова інвентаризація активів; 3) вибіркова документальна перевірка діяльності окремих посадових осіб чи менеджерів середньої ланки управління; 4) анкетування колективу підприємства з метою ідентифікації ризиків шахрайства
Моніторинг ризиків корупції та шахрайства	1) бліц-діагностика фінансового стану підприємства з використанням інструментарію вертикального та горизонтального (динамічного) аналізу; 2) оцінювання стану економічної надійності контрагентів, які потрапили до зони підвищеної уваги антикорупційного аудитора з використанням інструментів коефіцієнтного аналізу
Проведення службових розслідувань виявлених випадків корупції та шахрайства	1) запровадження «гарячої лінії»; 2) участь у атестації персоналу (перевірка на лояльність); 3) опитування свідків; 4) фактична перевірка; 5) пошук документальних доказів; 6)інформування колективу підприємства про факти виявлення корупційних схем та випадків шахрайства.
Оцінювання достовірності фінансової звітності та раннє діагностування маніпуляцій з фінансовими показниками	1) використання коефіцієнтного аналізу для оцінювання достовірності фінансової звітності; 2) використання методики оцінювання достовірності облікової інформації шляхом її порівняння з неофіційними даними, отриманими у результаті вживання спеціальних методів забезпеченні економічної безпеки.

Відтак вважаємо, що запровадження низки дисциплін, у яких розкриваються шляхи забезпечення економічної безпеки підприємства при підготовці фахівців з аудиту стане інноваційним кроком в галузі освіти та сприятиме модернізації вітчизняної економіки.

5.2. ЕКОНОМІЧНА ПРИРОДА ШАХРАЙСТВА З ФІНАНСОВОЮ ЗВІТНІСТЮ ТА СПОСОБИ ЙОГО ПОДОЛАННЯ

В умовах глобального ринку при прийнятті економічних рішень виникає необхідність у порівняльному аналізі та оцінці фінансового стану як національних, так і транснаціональних компаній. Для об’єктивного аналізу потрібна інформаційна платформа, в якості якої може бути використана фінансова звітність цих компаній, а уніфікованість та єдність інформаційної платформи може забезпечуватися конвергенцією національних та міжнародних стандартів фінансової звітності.

На підтвердження цієї тези слід нагадати той факт, що журнал Forbs при формуванні рейтингу 2000 найбільших світових компаній використовує чотири показники – ринкову капіталізацію, розмір виручки, прибутку та вартість активів. Причому три останні із них – бухгалтерські показники, джерелом інформації про які є фінансова звітність.

Формування раціонального потоку облікової інформації передбачає дотримання наступних принципів: об'єктивність відображення процесів фінансово-господарської діяльності, оперативність, точність і достовірність показників, що надаються. Недотримання цих принципів з метою спотворення фінансових даних призводить до утворення інформаційних ризиків прийняття менеджментом підприємства чи іншими групами стейкхолдерів необґрунтованих економічних рішень.

На сьогоднішній день маніпулювання фінансовими даними перетворилося на одну із найсуттєвіших загроз економічній безпеці як окремої компанії, так і держави де вона функціонує. Так за даними Всесвітнього огляду економічних злочинів у 2015 році частка економічних злочинів пов’язаних з фальсифікацією фінансових показників склала понад 30% усіх проявів економічної злочинності, що навіть перевищило такі традиційні види злодіянь як незаконне привласнення активів (23%) та відмивання грошей (21%) [1].

На підтвердження цього висновку слід зазначити, що 80% опитаних фінансових директорів провідних підприємств України відповіли, що їм доводиться маніпулювати фінансовими даними в професійній практиці [2].

Однак, незважаючи на суцільне розповсюдження маніпуляцій з фінансовими показниками, аналіз наукових публікацій дозволяє стверджувати, що в сучасних розробках теорії і методології інформаційного забезпечення бізнес-процесів в Україні відсутні дослідження пов'язані з визначенням впливу цього виду злочинів на стан економічної безпеки вітчизняних підприємств, які вимагають подальшого розгляду. Це потребує, у першу чергу, здійснення теоретичних досліджень економічної природи фальсифікацій фінансової звітності.

Узагальнення наукових поглядів на це явище дозволило сформулювати наступні точки зору щодо його сутності:

- це навмисне викривлення чи приховування істотних фактів господарської діяльності, які вводять користувача звітності в оману і в окремих випадках спонукають до зміни рішення, що приймається на основі фінансової звітності [3];

- це навмисні чи ненависні дії, або бездіяльність, що призводить до істотного спотворення показників фінансової звітності [4];

- використання бухгалтерського обліку для введення в оману користувачів, замість належної допомоги їм [5];

- зловживання методиками і принципами бухгалтерського обліку для досягнення фінансових результатів, які навмисно не забезпечують чесний і справедливий погляд на реальний характер речей [6];

- процес підготовки звітів підприємства так, щоб вони репрезентували його діяльність в найбільш сприятливому вигляді в очах акціонерів, інвесторів і інших зацікавлених осіб [7].

Підсумовуючи усі вказані погляди на сутність фальсифікацій з фінансовою звітність можемо зазначити, що головною метою здійснення фальсифікацій, як справедливо вважають Д. Александер і А. Бріттон [8], є “управління звітністю”, що призводить до помилкового сприйняття її користувачами. Як наслідок,

фальсифікація фінансової звітності наносить шкоду не лише широкому колу зовнішніх користувачів, але і внутрішнім користувачам фінансової інформації, зокрема, співробітникам та керівництву компанії. При цьому внутрішні користувачі несуть як фінансові, так і нефінансові втрати, наприклад втрату репутації. З іншого боку фальсифікація фінансової звітності може бути спрямована на приховування крадіжок цінностей скоєних співробітниками компанії, тобто носити неуправлінський характер.

Маніпулюючи даними фінансовій звітності, менеджери, з одного боку, націлені на здобуття вигод для підприємства і власника (управлінська фальсифікація), а, з іншою, – для себе (маніпуляції проти підприємства). При цьому М. Метьюс однією з причин виникнення неуправлінської фальсифікації звітності називає конфлікт між підзвітністю управління і завданням розподілу обмежених фінансових ресурсів [7]. Виконавцями неуправлінських фальсифікацій найчастіше виступають фінансові аналітики, головні бухгалтери, аудитори.

Дослідження сучасних проявів маніпулювання фінансовими показниками дозволяє зробити висновки, що в сучасних умовах:

- фальсифікація звітності є засобом вирішення масштабних завдань для менеджменту та власників;
- користувачами шахрайської звітності стають вже не одиниці та десятки, а тисячі та мільйони компаній;
- фальсифікація фінансової звітності набуває усе більш складних форм;
- паралельно зі зростанням управлінської фальсифікації звітності набуває обертів неуправлінська фальсифікація, тобто модель поведінки керівництва компанії неухильно переймається та копіюється співробітниками.

Узагальнення випадків прояву фальсифікації показників фінансової звітності на підприємствах України, дає можливість встановити основні причини маніпулювання обліковими даними, серед яких:

- *демонстрація інвестиційної привабливості*. Завищення прибутку з подальшою можливістю нарахування вищих дивідендів;

- *умовне підвищення кредитоспроможності*. Завищення прибутковості і заниження обсягів зобов'язань з метою здобуття вищої категорії позичальника при залученні кредитів;

- *отримання конкурентних переваг*. Маніпулювання даними фінансової звітності з метою здобуття більш високого рейтингу в галузі (регіоні);

- *зниження податкового тягаря*. Завищення витрат, що відносяться до базових, при оподаткуванні прибутку;

- *створення «запасу ефективності»*. Штучне поліпшення показників прибутковості, ліквідності, фінансовій стійкості з метою підвищення коефіцієнта фінансової надійності для потенційних партнерів;

- *протидія «недружньому» поглинанню*. Для створення перепони недружньому поглинанню керівництво навмисно спотворює фінансову звітність щоб сформувати невиправдані очікування інвесторів;

- *приховування фактів корупції*. Підтасовування фінансових показників для реалізації поставленої керівництвом мети: отримання державних замовлень, виділення земельних ділянок під забудову, отримання ліцензій тощо;

- *укриття фактів крадіжок активів*. Співробітники компанії з метою отримання додаткових матеріальних благ (привласнення активів) спотворюють дані бухгалтерського обліку та фінансової звітності.

Даний перелік причин дає можливість виділити три напрями отримуваних від цього вигід:

1) мінімізація витрат пов'язаних із сплатою податків, обов'язкових зборів, ресурсних платежів;

2) збільшення рейтингової оцінки іміджу підприємства;

3) максимізація виплат менеджерам;

4) незаконне привласнення активів у будь-який спосіб.

За даними асоціації незалежних сертифікованих бухгалтерів щорічно у світі збитки спричинені фальшуванням фінансової звітності складають 7% обороту компаній [9]. Схожа картина і в Україні, де за дослідженнями експертів 30% випадків

банкрутств підприємств супроводжувалося фальшуванням облікових даних, відображених у звітності.

При цьому вони стверджують, що до 2008 року технології управління звітністю стосувалися лише:

- управління прибутком у Звіті про фінансові результати (звіті про сукупний дохід) та податковій декларації з податку на прибуток;
- управління структурою активів і капіталу в Балансі (звіті про фінансовий стан).

Однак, практика ведення бізнесу українськими підприємствами в кризових умовах засвідчила, що фальшування даних вже застосовується і до коректування грошових потоків в Звіті про рух грошових коштів.

У сучасній економічній літературі розглядаються різні методи і прийоми фальшування облікових даних, які можна узагальнити в три основні групи:

1) вибір облікових оцінок;

2) вибір і вживання методів бухгалтерського обліку;

3) формальне відображення господарських операцій всередині однієї фінансово-промислової групи;

4) вибір стандартів бухгалтерського обліку і фінансової звітності.

Облікові оцінки застосовуються для максимізації, мінімізації, або вирівнювання прибутку шляхом перерозподілу витрат між звітними періодами. На практиці з цією метою найчастіше використовують завищення резерву сумнівних боргів. Наприклад, українською енергетичною компанією ДП НАЕК “Енергоатом” з метою мінімізації прибутку станом на 1 січня 2008 року був нарахований резерв сумнівних боргів в сумі 2,1 млрд. грн., що склало 42% загальної суми витрат 2007 року [10].

Методи бухгалтерського обліку охоплюють визнання, оцінку і розкриття інформації у фінансовій звітності. При використанні цих методів зазвичай застосовують професійні судження, діапазон яких може бути достатньо широким. Найчастіше, як стверджує В. Елліот [11], фальшування облікових показників пов'язане з маніпуляціями у відображенні запасів. Спираючись на

аналіз звітності публічних компаній США, він виділяє наступні фіктивні операції, пов'язані з обліком запасів: включення в активи застарілих запасів, що підлягають списанню; відображення запасів у складі збитків; суб'єктивізм при визначенні чистої вартості реалізації запасів і розподілі виробничих накладних витрат.

Ще одним проявом творчості в обліку є здійснення формальних операцій між підприємствами в середині фінансово-промислових груп, що знайшло широке розповсюдження у вітчизняній практиці. Для цього власниками створюється значна кількість юридичних осіб, які здійснюють операції між собою. Така схема дозволяє фінансово-промисловій групі маніпулювати прибутком та укривати значні боргові зобов’язання, а підприємствам, що до неї входять виглядати в кращому світлі в очах потенційних партнерів.

Інтеграція українських підприємств в міжнародний економічний простір пов'язана з появою ще одного напряму фальшування облікових даних, спричиненого застосуванням різних методологічних підходів до обліку окремих операцій за національними і міжнародними стандартами фінансової звітності. Показовим в цьому контексті є випадок з транспортною корпорацією “Укрзалізниця”, про яку в українській пресі поширилася інформація, про те, що за даними міжнародного аудиту ця корпорація за результатами 2007 року мала збитки у розмірі 3,5 млрд. грн. замість раніше задекларованого прибутку в сумі 707 млн. грн. Як пояснило керівництво корпорації, збитковий фінансовий результат був показаний у фінансовій звітності, складеній за правилами міжнародних стандартів. Таким чином, вказані розбіжності у фінансовому результаті з'явилися не внаслідок приховування прибутку, а лише завдяки розбіжностям в методології ведення обліку у вітчизняній та зарубіжній практиці [10].

Відтак, використання міжнародних стандартів фінансової звітності в якості важеля підвищення рівня корпоративної прозорості українських компаній не лише не призвело до уникнення випадків фальшування, але і стало одним із

найулюбленіших прийомів «творчого відношення» до формування звітних показників.

В цілому можна виокремити три рівні корпоративної прозорості при оприлюдненні фінансових даних вітчизняними підприємствами.

Перший рівень прозорості характерний усім підприємствам, які на вимогу вітчизняного законодавства повинні оприлюднювати фінансову звітність. Однак, ні для кого не секрет, що довіра користувачів до даних представлених у звітності уже давно є дуже низькою. І не важливо в якому форматі вона надається – за українськими правилами ведення обліку чи міжнародними.

Другий рівень прозорості позиціонують компанії, які публічно розкривають свою стратегію розвитку, суму вкладених інвестицій та рівень дохідності. Однак, як показує практика, зазначені показники у їх фінансовій звітності також не вирізняються високим рівнем достовірності.

З найбільшою обережністю слід відноситися до звітності крупних вітчизняних сировинних компаній з наступних причин. Зазвичай ці компанії отримують високі прибутки і для ухилення від їх оподаткування підтасовують оподатковувану базу. По-друге, саме в сировинних компаніях найбільше зацікавлені іноземні інвестори, відтак для підвищення привабливості відбувається фальшування фінансових даних. По-третє, фальшування даних звітності може відбуватися і як протидія «недружньому» поглинанню з метою уникнення рейдерських захоплень.

Третій рівень прозорості характерний для середніх підприємств. Зазвичай саме такі підприємства найбільше зацікавлені в залученні інвестицій, а відтак їх керівництво вважає за доцільне надати якомога більше інформації про свій бізнес. Окрім того, зважаючи на невеликий масштаб таких підприємств, серйозні порушення у їх фінансовій звітності можуть бути легко виявленими, тому підприємства не ризикують фальшувати дані звітності.

Також можна простежити рівень корпоративної прозорості і за галузевою приналежністю підприємств. Зокрема, найвищим рівнем прозорості в Україні характеризуються підприємства телекомунікацій (59% прозорості інформації) та

виробники соків і молочної продукції (52% прозорості інформації). В той же час середній показник розкриття фінансової звітності українських підприємств не перевищив 25%, що значно нижче європейських стандартів.

Низький рівень прозорості розкриття фінансової інформації та суцільне поширення випадків маніпуляцій з показниками звітності зумовило пошук шляхів для запобігання цьому явищу. Традиційно вважається, що боротися із спотвореннями фінансової інформації повинен незалежний аудитор. Проте, дані, отримані в результаті дослідження, проведеного американською аналітичною компанією Weiss Ratings, підтверджують, що зв'язок між позитивною оцінкою аудиторів та реальними перспективами компанії досить умовний. Так у 2008 році було виявлено 42% крупних компаній, що визнали себе банкрутами менш ніж за рік після отримання ними позитивного аудиторського висновку [12, с. 43]. При цьому у більшості цих компаній аудиторами були представники фірм KPMG, Ernst&Young, PricewoterhouseCoopers, Deloitte & Touche, що входять до топ-четвірки всесвітньо відомих аудиторських компаній.

Така ж картина простежується і в Україні. Як показує український досвід господарювання, практично вся недостовірна фінансова звітність крупних компаній мала позитивні аудиторські висновки. Прагнучи максимізувати свій прибуток, аудиторські фірми нерідко порушують як етичні, так і законодавчі норми. У цьому контексті слід згадати випадки з національною банківською системою, що отримали широкий розголос, коли в аудиторських висновках, які надавалися зовнішніми аудиторами була підтверджена недостовірна фінансова звітність, яка істотно спотворювала реальний фінансовий стан [13, с. 67].

В зв’язку з цим, можна стверджувати, що обов’язкова аудиторська експертиза фінансової звітності не є панацеєю при упередженні наслідків фальшування фінансових показників.

На наш погляд, дослідницький ракурс при вирішенні цієї проблеми має бути спрямований в площину безпосередніх користувачів інформації, яким

необхідно розробляти внутрішні механізми перевірки достовірності фінансової звітності потенційних партнерів або інших контрагентів з метою:

- діагностування їх реального фінансово-господарського стану щоб уникнути загрози співпраці з потенційним банкрутом;
- підготовки інформації для ухвалення управлінських рішень відносно співпраці з партнерами в умовах виявлених загроз і небезпек;
- максимально повного інформаційного забезпечення системи економічної безпеки власного підприємства.

Для раннього діагностування маніпуляцій з фінансовими показниками та упередження наслідків прояву цього виду економічних злочинів М. Беніш запропонував використовувати методи фінансового аналізу та запропонував «Карту нормативних відхилень фінансових індикаторів» [14, с. 35]. В основу карти було покладено перелік фінансових індикаторів, які на думку автора з найвищою точністю дозволяли оцінити рівень маніпулювання фінансовими показниками і могли бути розрахованими за даними фінансової звітності.

До складу ключових фінансових індикаторів, які використовуються для виявлення фальсифікації фінансової звітності увійшли:

- темп зростання виручки від реалізації;
- темп зниження маржинального доходу (валового прибутку) у виручці від реалізації;
- темп зростання якості активів (частки необоротних активів у структурі активів підприємства);
- темп зміни (різкого зростання чи падіння) оборотності дебіторської заборгованості;
- темп зниження фінансового важеля.

При виявленні у звітності компанії-контрагента різкого *зростання темпів виручки від реалізації* слід звернути увагу на те, що така компанія скоріш за все знаходиться в групі підвищеного ризику, оскільки зростання обсягів продажу потребує залучення додаткового фінансування.

Темп зниження частки маржинального доходу у виручці від реалізації свідчить про те, що дохідність компанії знижується і, як наслідок, погіршуються її перспективи на ринку. При цьому даний показник потрібно аналізувати у порівнянні з показником «Темп зростання виручки від реалізації». Якщо виручка від реалізації зростає, а маржинальний дохід у ній знижується, це свідчить про ознаки фальшування зазначених показників.

При виявленні *темпів зростання якості активів (необоротних активів у загальній сумі активів)* компанії слід звернути увагу на те, що її спроможність генерувати грошові потоки у цьому випадку знижується. Зростання необоротних активів не пов'язане зі зростанням основних засобів скоріш за все свідчить про невиправдану капіталізацію витрат, що спричиняє умовне завищення прибутку звітного періоду.

Різкі *зміни терміну оборотності дебіторської заборгованості* є підставою для констатації факту маніпуляцій з фінансовими показниками, адже за умови стабільного бізнесу та незмінної договірної політики показник оборотності дебіторської заборгованості буде залишатися практично на одному рівні. Відтак, у випадку різкого зростання оборотності дебіторської заборгованості велика імовірність того, що здійснюються маніпуляції з розміром виручки від реалізації. Якщо ж показник оборотності дебіторської заборгованості різко знизився, можливим є штучне завищення розміру дебіторської заборгованості при незмінному розмірі виручки від реалізації.

Про шахрайство зі звітними показниками буде свідчити й різке зниження *фінансового важеля*, що характеризує кредитний ризик, якому піддається компанія. Оскільки ринкова вартість акцій компанії залежить від рівня фінансового важеля її керівництво з метою підвищення ринкової вартості акцій може штучно знижувати рівень фінансового важеля за рахунок включення кредиторської заборгованості до складу витрат.

Однак, навіть чітке здійснення моніторингу індикаторів М. Беніша з метою оцінювання рівня шахрайства з фінансовими показниками на думку самого

автора дозволяє виявити лише 50% випадків фальсифікації фінансової звітності [14, с. 36].

Відтак виникає необхідність у запровадженні додаткового комплексу заходів, які, на наш погляд, стосуються в першу чергу діяльності в системі безпеки компанії, які б надавали можливість виявити інші (відмінні від фінансових) фактори ризику фальшування показників звітності.

До таких факторів відносять:

1. Систему корпоративного управління. При цьому слід звертати увагу на часті зміни організаційної структури, децентралізовану систему управління, відсутність служби внутрішнього контролю.

2. Кадровий склад та репутацію керівництва компанії. Ознаками можливого шахрайства у звітності може бути часта зміна топ-менеджменту компанії, родинні чи дружні зв'язки між ними, негативна ділова репутація керівників компанії.

3. Взаємодію із зовнішніми аудиторами. Фальшування звітності зазвичай здійснюють компанії, для яких характерна часта ротація зовнішніх аудиторів, розташування підрозділів у важкодоступних для аудиторів місцях (наприклад на території закритих територіальних утворень).

Для виявлення цих факторів та встановлення достовірності звітних даних що надходить, як із зовнішніх джерел (для уникнення наслідків управлінської фальсифікації), так і від бухгалтерської служби усередині підприємства (для недопущення прояву неуправлінської фальсифікації) слід застосовувати у практичній діяльності фахівців з безпеки способи отримання альтернативних даних.

Альтернативна інформація може бути отримана з офіційних джерел, серед яких найбільш поширеними є:

- висновки незалежних аудиторських компаній;
- видання центральних і регіональних органів управління статистики України. У них надаються середньогалузеві показники за окремими напрямами діяльності;

- періодичні офіційні видання державних органів і структур, видання Державної комісії з цінних паперів і фондового ринку, відомчі збірки, які містять інформацію про фінансові та економічні показники;

- офіційні сайти державних структур, комітетів і міністерств, на яких публікується річна фінансова звітність;

- біржова інформація про динаміку змін вартості цінних паперів і тенденцій на фондовому ринку в цілому і за окремими сегментами.

Окрім цього достовірність наданої облікової інформації можна оцінити і шляхом її порівняння з неофіційними даними, отриманими у результаті вживання спеціальних методів забезпеченні економічної безпеки. Серед них основними є: метод конфіденційних стосунків, метод особистого пошуку, метод спеціалізованого опитування, метод конфіденційного спостереження.

Перевіреній належним чином обліковій інформації присвоюється коефіцієнт достовірності, який показує її вплив на подальші наслідки при прийнятті на основі цієї інформації управлінських рішень відносно ділової співпраці з тим або іншим контрагентом (таблиця 5.3).

Таким чином, проведені дослідження засвідчують, що запровадження запропонованої методики перевірки достовірності облікової інформації в практичну діяльність вітчизняних копаній підвищить аналітичні можливості фінансової діагностики та забезпечить здійснення багаторівневого системного моніторингу звітної інформації, що сприятиме зниженню інформаційного ризику для користувачів облікових даних в умовах зростаючої ролі шахрайства з фінансовою звітністю.

Таблиця 5.3

Ранжування облікової інформації залежно від ступеня її достовірності

Значення коефіцієнта в шкалі достовірності	Розшифровка вимог (характеристик), що підтверджують достовірність інформації
1,0	Інформація, що міститься у фінансовій звітності достовірна, підтверджена спеціальними методами перевірки, офіційними повідомленнями органів влади, отримана безпосередньо у її власника, який не має мотивів спотворювати достовірність цієї інформації.
0,9	Інформація, що міститься у фінансовій звітності в цілому відповідає дійсності, підтверджена спеціальними методами перевірки, надана з дозволу керівництва підприємства, але відсутнє офіційне зовнішнє підтвердження її достовірності.
0,8	Інформація, що міститься у фінансовій звітності практично відповідає дійсності, що підтверджується висновком незалежного аудитора та спеціальними методами перевірки. Вона отримана у відповідності до розпорядження керівництва підприємства, але у аналітика не має впевненості, що особи, які її готували володіють достатньою кваліфікацією та навичками, здатними задовольнити специфічні потреби користувачів цієї інформації, тому її достовірність викликає сумнів.
0,7	Надана контрагентом (менеджером окремого сегменту в середині підприємства) інформація містить невідповідності з показниками офіційної фінансової (внутрішньої) звітності, вона підготовлена без належного контролю з боку керівництва контрагента (менеджера окремого сегменту), який не має наміру показувати правдиву інформацію, крім того існує негативна зовнішня інформація про цього контрагента (внутрішній сегмент діяльності).
0,6	Надана інформація про контрагента носить орієнтовний характер, не має підтвердження її достовірності з боку офіційних зовнішніх джерел, разом з тим, перевірка спеціальними методами, мотивів надання неправдивої інформації з боку керівництва цього контрагента не виявила.
0,5	Інформація про контрагента носить неповний характер і базується лише на даних фінансової звітності, частково підтверджена даними нефінансового характеру, отриманими за запитом, але спеціальними методами перевірки не встановлено її достовірність.
0,4	Інформація надана в фінансовій звітності контрагента носить невизначений характер, її достовірність не підтверджена спеціальними методами перевірки, а альтернативні джерела інформації не утримують даних про діяльність цього підприємства.
0,3	Фінансова інформація надана контрагентом з метою введення в оману керівництво підприємства при визначенні пріоритетів співпраці з ним, вона носить дезінформаційний характер, її показники в основному не відповідають дійсності, що підтверджено спеціальними методами перевірки, але вони ідентичні показникам оприлюдненої фінансової звітності цього контрагента.
0,2	Фінансова інформація, надана контрагентом (менеджером окремого сегменту) з метою введення в оману керівництво підприємства, носить дезінформаційний характер, фінансові показники не відповідають дійсності, що підтверджено спеціальними методами перевірки.
0,1	Інформація про контрагента відсутня, на запити щодо її отримання керівник підприємства не відповідає.

5.3. МАНІПУЛЮВАННЯ ОБЛІКОВИМИ ДАНИМИ ЯК СКЛАДОВА ПРОФЕСІЙНОГО РИЗИКУ БУХГАЛТЕРА

Ризики характерні усім сферам людської діяльності - не винятком є і діяльність пов’язана із веденням бухгалтерського обліку. На думку фахівців з економічної безпеки до найсуттєвіших загроз, спричинених професійним ризиком бухгалтера, відносять недостовірність облікової інформації в результаті навмисного чи ненавмисного спотворення її обліковим персоналом, або недосконалості методичного інструментарію при забезпеченні інформаційних потреб економічної безпеки [15].

Високий ступінь ризику в професійній діяльності бухгалтера та його відповідальність перед користувачами облікової інформації потребує визнання в системі професійних ризиків підприємства категорії “професійний ризик бухгалтера” та розроблення економічної політики щодо управління ним.

Дослідження сутності та природи утворення професійних ризиків, пов’язаних з кругообігом облікової інформації, здійснено у працях таких вітчизняних та зарубіжних вчених як Л. Бернстайн [16] Л.Чижевська та І.Вигівська [17], О. Шевельов [18] та інших. Разом з тим, мусимо наголосити, що у своїй більшості ці дослідження носять різноплановий характер і потребують систематизації з позицій управління професійним ризиком бухгалтера в системі економічної безпеки.

Під *професійним ризиком бухгалтера* розуміють інформаційні ризики пов'язані зі спотворенням облікових даних, які виникають у системі бухгалтерського обліку і є наслідком дій або бездіяльності облікового персоналу. Першопричиною виникнення цих ризиків є "… фактор людської природи, а також неточності, властиві основним процесам обліку. Вони мають місце через наявність альтернативних принципів обліку та нечітких стандартів щодо їх застосування, що спричиняє значний ступінь невизначеності" [16, с. 56].

Узагальнений склад факторів, що впливають на виникнення професійних ризиків бухгалтера надано в таблиці 5.4.

В умовах сьогодення бухгалтер є активним учасником процесу управління. Він повинен володіти навичками аналітичної роботи, здійснювати контроль за якістю ведення обліку, добре знати новітні інформаційні системи, податкове та трудове законодавство. При цьому праця бухгалтера носить в певному сенсі творчий характер.

Таблиця 5.4

Склад факторів, що впливають на виникнення професійних ризиків пов'язаних зі спотворенням облікових даних

Джерело утворення ризику	Склад факторів, що спонукають виникнення інформаційних ризиків
Організація праці працівників бухгалтерії	Недостатній рівень знань керівників бухгалтерської служби, що не дозволяє їм організувати ефективну обліково-інформаційну систему підприємства
	Недостатній професійний рівень бухгалтерів
	Витік конфіденційної інформації з вини співробітників бухгалтерії
Методика ведення бухгалтерського обліку	Порушення принципів та правил ведення бухгалтерського обліку
	Невдалий вибір способів обліку, регламентованих стандартами бухгалтерського обліку та фінансової звітності
Організація та технологія ведення бухгалтерського обліку	Неефективна політика підприємства з організації бухгалтерського обліку
	Застарілі інформаційні технології, що не відповідають сучасним вимогам обробки, збереження та надання облікової інформації окремим групам користувачів

Це пояснюється, по-перше, відносно широкою свободою вибору способів ведення обліку, що потребує професійного судження бухгалтера. По-друге, необхідністю задоволення широкого кола зовнішніх користувачів, які вимагають різноманітної за своїми характеристиками та складом інформації. По-третє, тиском з боку власників підприємства, які прагнуть мінімізувати свої витрати пов'язані зі сплатою податків та інших соціальних зборів.

Виконання зазначених вимог супроводжується існуванням трьох основних груп професійних ризиків бухгалтера: ризики пов'язані з порушенням методики ведення бухгалтерського обліку, організаційні ризики та ризики навмисного спотворення інформації.

1. Ризики пов'язані з порушенням методики ведення бухгалтерського обліку в результаті необґрунтованого вибору облікової політики. Виникнення даної групи ризиків пов'язане у першу чергу з недосконалою кваліфікацією бухгалтера при застосуванні ним професійного судження. Професійне судження бухгалтера носить суб'єктивний характер, оскільки це думка заснована на знаннях, вмінні та досвіді окремого фахівця, які не завжди отримані ним у повній та достатній мірі. Відтак, критерієм правильності професійного судження бухгалтера є достовірність фінансової звітності та мінімізація наслідків інформаційного ризику. В той час як некваліфіковане професійне судження призводить до формування облікової інформації, що не володіє якостями, необхідними менеджменту для ефективного управління діяльністю підприємства, а оприлюднена фінансова звітність спонукає зовнішніх користувачів до прийняття на її основі рішень не вигідних для підприємства.

2. Організаційні ризики пов'язані з тим, що структура бухгалтерської служби, організація облікової роботи, кваліфікація та інші професійні та особистісні характеристики працівників не відповідають завданням, поставленим перед апаратом бухгалтерії. Це може призвести до зростання трудомісткості і зниження оперативності облікової роботи, невиправданого збільшення штату бухгалтерії і, відповідно, падіння ефективності системи бухгалтерського обліку. Крім того, до цієї ж групи ризиків доцільно віднести ризики втрати конфіденційної інформації внаслідок недбалості або злого наміру працівників бухгалтерії.

3. Ризики спотворення інформації. У цю групу відносяться ризики порушення персоналом бухгалтерської служби законодавчих (нормативно-правових) актів, які регулюють фінансово-господарську діяльність підприємства, що спричиняє викривлення достовірності облікової інформації.

При цьому, якщо раніше фальшування облікових даних здійснювалося зазвичай на вимогу керівництва та власників підприємства, за останні два роки, як підтверджують результати досліджень [19, ст.13], частка маніпулювань

фінансовими показниками здійснена обліковими категоріями персоналу з метою отримання додаткових вигод для себе склала 24% від загальної суми зафіксованих випадків спотворення фінансової звітності.

Суцільне розповсюдження фальшування показників фінансової звітності зумовило пошук шляхів для подолання цього явища. В зв'язку з цим перед вітчизняними підприємствами стоїть нагальна проблема розробки внутрішніх механізмів упередження, оцінки та зниження професійних ризиків властивих обліковій системі, які повинні бути покладені в основу їх економічної політики (рис. 1).

Метою функціонування механізму упередження професійних ризиків бухгалтера є недопущення виникнення негативних тенденцій спричинених діяльністю облікового персоналу, пов'язаною з навмисним чи ненавмисним маніпулюванням обліковими даними; своєчасне виявлення нелояльно настроєних до підприємства осіб; забезпечення надійного захисту комерційної таємниці підприємства; протидія комерційному шпигунству тощо.

У зв'язку з тим, що найменш прогнозованими при встановленні імовірності виникнення є ризики пов'язані зі спотворенням облікової інформації, їх достовірна та об'єктивна оцінка в системі бухгалтерського обліку - утруднена. Відтак, підмурком механізму такого оцінювання має стати імплементація в систему бухгалтерського обліку спеціальних методів та прийоми, що застосовуються спеціалістами з безпеки (про що йшла мова в параграфі 2 цього розділу).

Не менш важливим аспектом, що потребує запровадження процедур перевірки з боку фахівців служби економічної безпеки є обґрунтований підбір кадрового потенціалу бухгалтерії з метою мінімізації ймовірних негативних наслідків професійних ризиків. Таку перевірку доцільно здійснювати за кожною особою при її прийомі на роботу, за групою спеціалістів бухгалтерії, що займаються наданням інформації за окремими перспективними напрямами діяльності перед проведенням найбільш важливих угод за їх участі та при встановленні ступеню дотримання ними комерційної таємниці, а також в цілому по підрозділу бухгалтерії, якщо перевірка носить плановий характер

(раз на рік). Випробування виконується за наступними напрямами: лояльність, чесність в роботі, компетентність та дотримання комерційної таємниці.

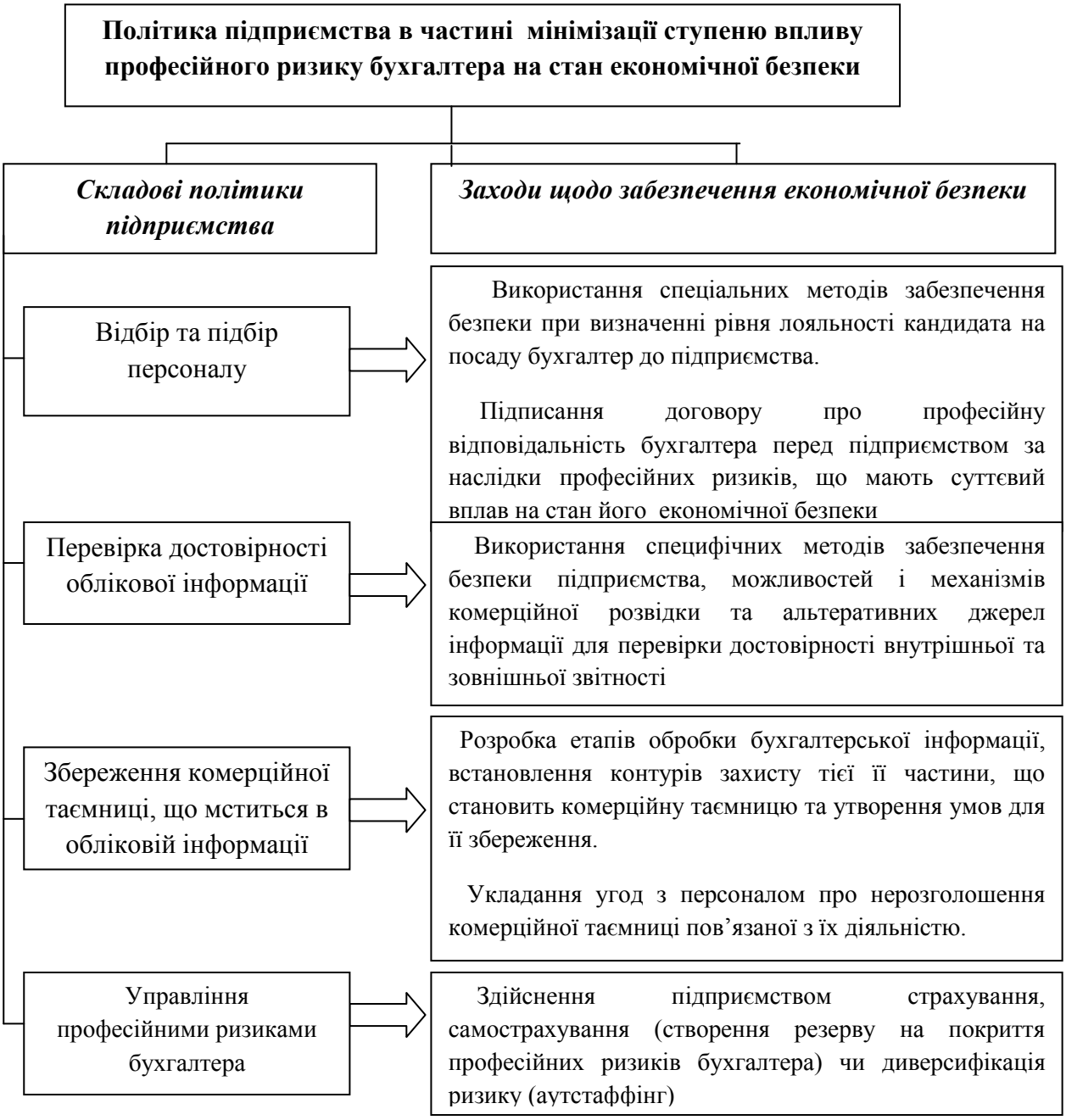


Рис. 5.1. Політика підприємства в частині управління професійними ризиками бухгалтера

Лояльність дає можливість перевірити бухгалтера щодо його готовності:

- надавати інформацію керівництву про можливі вигідні контракти, про діяльність конкурентів;

- бережно ставитися до майна підприємства;

- підтримувати та укріплювати здоровий морально-психологічний клімат на підприємстві взагалі та в бухгалтерії зокрема.

В основу перевірки облікового персоналу на лояльність покладено метод професійного спостереження та метод спеціальних психофізіологічних та психологічних досліджень.

Метод спостереження дозволяє виявити контакти бухгалтера, які можуть свідчить про можливість його нелояльної поведінки до свого підприємства. При цьому категорично забороняється використовувати отриману інформацію з метою шантажу працівника чи порушувати його конституційні права при здійсненні професійного спостереження.

Метод спеціальних психофізіологічних та психологічних досліджень передбачає отримання достовірної інформації про особу з використанням спеціальних психологічних, психофізіологічних та інформаційних пристроїв. В основі методу лежать принципи психологічного тестування або проведення перевірки із застосуванням поліграфу (детектора брехні), що дають можливість виявити інформацію стосовно можливих нелояльних дій, яку особа приховує, виходячи з її психологічної структури особистості.

Основний зміст перевірки на чесність в роботі полягає в тому, що бухгалтеру, якого перевіряють, створюють умови, при яких він може зчинити шахрайські дії, будучи впевненим, що їх не викриють. Перевірці на чесність, зазвичай, підлягають наступні операції:

- отримання комісійних («відкатів») від партнера. При цьому партнер діє за згодою з керівником підприємства про взаємну перевірку кадрів;

- завищення грошових коштів, виданих під звіт працівникам, з якими вступив бухгалтер у зговір з можливим «відмиванням» їх певної частки;

- несанкціоноване використання грошових коштів в касі на власні потреби з наступним поверненням;

- використання грошей підприємства для спекуляцій з валютою;

- використання автотранспортних засобів для особистих потреб, тощо.

Перевірка професійної придатності та компетентності, зазвичай проводиться головним бухгалтером чи його замісником, а в разі, якщо суб'єктом перевірки є здобувач посади головного бухгалтера, то фінансовим директором підприємства. Перевірка проводиться: шляхом співбесіди за проблематикою бухгалтерського обліку чи доручення виконати ту або іншу роботу, наприклад скласти звітність, заповнити первинний документ тощо.

При перевірці на дотримання комерційної таємниці у сферу уваги повинна потрапити:

- перевірка випадків зривів контрактів за участі бухгалтера;
- випадки втрати бухгалтером документів, що містять комерційну таємницю на попередніх місцях його роботи;
- випадки роботи із секретними документами підприємства вдома або у вечірній (неробочий) час без узгодження з керівництвом;
- випадки перехоплення конкурентами угод, контрактів, про які було відомо бухгалтерові.

Контроль за дотриманням комерційної таємниці в поточній діяльності бухгалтера здійснюється за допомогою спеціального програмного забезпечення (McAfee Host Data Loss Prevention, McAfee Network DLP, Symantec Data Loss Prevention, Websense Data Security Suite (DSS), Контур информационной безопасности), що дозволяє фахівцям з безпеки контролювати проходження та розповсюдження облікової інформації, яка відноситься до комерційної таємниці або до інформації з обмеженим доступом.

За кожним з вказаних напрямів перевірки облікового персоналу здійснюється оцінка ймовірності виникнення професійного ризику, що визначається в балах від 0 до 100. Це дає можливість аналітику з питань фінансово-економічної безпеки розрахувати узагальнюючий коефіцієнт рівня професійного ризику бухгалтера як середньоарифметичної величини за формулою:

$$\boldsymbol{P = \sum Q : N} \qquad (1),$$

де P – професійний ризик бухгалтера;
Q - сума набраних балів за усіма складовими перевірки;
N - кількості напрямів перевірки.

В залежності від значення даного показника аналітик визначає чотири рівні впливу професійного ризику бухгалтера на стан економічної безпеки підприємства: мінімальний вплив ризику (0-25 балів), несуттєвий вплив ризику (26-49 балів), суттєвий вплив ризику (50-89 балів), катастрофічний вплив ризику (90-100 балів) та дає рекомендації стосовно управління ним.

Зважаючи на те, що наслідки професійного ризику бухгалтера пов'язані для підприємства лише з можливими втратами або отриманням нульового результату, при їх управлінні не розглядається перспектива виявлення шляхів отримання позитивного результату, а лише ставиться мета мінімізації імовірних збитків. Разом з тим, при виборі стратегії управління професійними ризиками слід виходити з того, що додаткові витрати пов'язані з мінімізацією негативних наслідків ризику не повинні перевищувати вигоди спричинені такою мінімізацією.

Тому при виявленні *мінімального ризику* не здійснюються дії щодо його управління, оскільки наслідки такого ризику характеризуються як незначні і не призводять до втрати капіталу підприємства.

При встановленні *несуттєвого професійного ризику* бухгалтера найбільш доцільним для підприємства буде створення внутрішнього резерву для виконання зобов'язань за цим ризиком, що не потребуватиме попереднього відволікання грошових коштів з підприємства, а їх реальне вибуття здійснюватиметься на момент фактичного прояву наслідків ризику.

При встановленні *критичного професійного ризику* доцільною буде його диверсифікація. Найпродуктивнішим видом диверсифікації на сьогоднішній день є аутстаффінг. З метою мінімізації кадрових ризиків в системі бухгалтерського обліку під аутстаффінгом розуміють послугу з виведення облікового персоналу за штат підприємства та оформлення його в штат компанії-провайдера. Провайдер бере на себе обов'язки виконання окремих видів облікових робіт, а відповідно і ризики пов'язані з таким виконанням, що дає можливість подолати три основні проблеми:

- по-перше, велика кількість неврегульованих законодавчих актів в галузі бухгалтерського обліку потребує від бухгалтерів відповідних знань та логіки

мислення, що не завжди відповідає рівню їх кваліфікації, а отже породжує ризик недостовірності облікових даних та низької продуктивності праці. Тому провайдер бере на себе ризик правильної інтерпретації найбільш неврегульованих питань та їх документально-юридичного супроводу;

- по-друге, більшість малих та середніх підприємств не може дозволити собі надання своїм співробітникам соціальних пільг у зв'язку з їх значною вартістю. Це породжує конфлікт інтересів між підприємством та його обліковими фахівцями, що викликає ризик маніпуляцій з фінансовими показниками, тому провайдер бере на себе відповідальність за зниження соціальних суперечностей;

- по-третє, висококваліфіковані облікові спеціалісти, зазвичай, диктують підприємству завищені вимоги щодо оплати чи умов своєї праці, задовольнити які роботодавцю важко в силу певних причин. Тому провайдер бере на себе ризик конфліктних ситуацій, а підприємство при цьому отримує кваліфікованого фахівця.

При встановленні *катастрофічного впливу професійного ризику* бухгалтера підприємству слід обрати один із варіантів дій:

- уникнення ризику, тобто усвідомлену відмову від співпраці з окремим працівником чи категорією облікового персоналу, діяльність яких може спричинити суттєві збитки підприємству;

- страхування ризику. У цьому випадку підприємство підписує договори про страхування відповідальності за заподіяні збитки з найбільш ризико-небезпечними категоріями облікового персоналу (студентами, спеціалістами низької кваліфікації, пенсіонерами, особами, за якими встановлено випадки порушення комерційної таємниці на попередніх місцях роботи тощо) та визначає розмір страхових внесків, що сплачуються страховій компанії. Укладання договору страхування професійної відповідальності забезпечить впевненість у відшкодуванні втрат та уможливить уникнення підприємством фінансових проблем. Таким чином, сформовані страхові фонди є своєрідною гарантією погашення наслідків професійних ризиків.

Однак, як зазначають окремі дослідники [17, с. 202], страхування професійної відповідальності як метод управління професійними ризиками бухгалтера не знайшов широкого розповсюдження в страховій практиці України та відповідно в діяльності вітчизняних суб'єктів господарювання. Менше ніж 50% досліджених страхових компаній України пропонують послуги страхування професійного ризику бухгалтера, що пов'язано з відсутністю чіткої регламентації даного питання на рівні законодавства та низьким рівнем розвитку страхової діяльності в країні.

Таким чином, проведені дослідження засвідчують нагальну необхідність розробки та запровадження в практичну діяльність вітчизняних суб'єктів господарювання механізмів взаємодії облікової системи та системи економічної безпеки в частині управління професійним ризиком бухгалтера. Головними інструментами такої взаємодії виступають спеціальні методи перевірки, властиві економічній безпеці, які використовуються при встановленні імовірності настання професійних ризиків бухгалтера, з метою: недопущення виникнення негативних тенденцій спричинених діяльністю облікового персоналу, пов'язаною з навмисним чи ненавмисним маніпулюванням обліковими даними; своєчасного виявлення нелояльно настроєних до підприємства осіб; забезпечення надійного захисту комерційної таємниці підприємства; протидії комерційному шпигунству тощо.

Доведено, що основними методами управління професійним ризиком бухгалтера є диверсифікація, резервування та страхування професійного ризику. Використання того чи іншого методу залежить від ступеня ризику, причини його виникнення та прийнятого керівництвом підприємства рішення щодо мінімізації чи нейтралізації ризику.

Список використаних джерел:

1. *Всесвітній огляд економічних злочинів [Електронний ресурс] : за даними міжнародної консалтингової агенції PwC. – Режим доступу: www.pwc.com\ua*
2. *Творчі аспекти фінансової звітності // Вестник бухгалтера и аудитора Украины. – 2003. - №23. – с. 2.*
3. *Association of Certified Fraud Examiners. Cooking the Books: What Every Accountant Should Know About the Fraud. Self-Study Workbook: Austin, TX, 2007/ - №91 – 5201. – P. 8*

4. Thorhill W.T., Wells J.T. Fraud terminology Reference guide. Association of Certified Fraud Examiners, Austin, TX, - 1993. - P. 28
5. Parker R. H. Macmillan Dictionary of Accounting / R. H Parker. – [Second Edition]. – London: The Macmillan Press Ltd., 1992. – 307 p.
6. O'Regan P. Financial Information analysis / P. O'Regan. - [Second Edition]. – Chichester: John Wiley&Sons Ltd., 2006. – 595 p.
7. Мэтьюс М.Р. Теория бухгалтерского учета / М.Р. Мэтьюс; пер. с англ. Э. И. Гогия; под ред. Я.В. Соколова, И.А. Смирновой. – М., 1999. – 663 с.
8. Александер Д. Международные стандарты финансовой отчетности: от теории к практике / Александер Д., Бриттон А.; пер. с англ. В.И. Бабкиной, Т.В. Седовой. – М., 2005. – 768 с.
9. 2008 Report to the Nation on Occupational Fraud and Abuse, ACFE. URL: http: // www.acfe.com/ rttn
10. Голов С. Креативный учет – угроза профессии и обществу/ С. Голов // Бухгалтерский учет и аудит. – 2011. - №1. – с. 31-43.
11. Elliot B. Financial Accounting and Reporting / B. Elliot, J. Elliot. - [Tenth edition]. – Edinburgh: Pearson, 2006. – 867 p.
12. Сотникова Л.В. Мошенничество с финансовой отчетностью: выявление и предупреждение / Л.В.Сотникова. – М.: Изд-во «Бухгалтерский учет», 2011. – 208 с.
13. Бутинець Ф.Ф. Альфа і омега бухгалтерського обліку, або моя болісна несповідь / Ф.Ф. Бутинець. – Житомир: ЖДТУ, 2007. – 328 с.
14. Beneish M. D. Detection of Earnings Manipulation // Financial Analyst Journal. – 1999. - №5. – P. 22-36
15. Анкета для дослідження організації та здійснення обліково-аналітичного забезпечення функціонування системи економічної безпеки суб'єктів господарської діяльності. - Київ: УСПП, 2010. - 14 с.
16. Бернстайн Л.А. Анализ финансовой отчетности: теория, практика и интерпретация: перевод с англ. / Науч. ред. перевода чл.-корр. РАН И.И. Елисеева. Гл. редактор серии проф. Я.В. Соколов. - М.: Финансы и статистика, 1996. - 624 с.
17. Професійна діяльність бухгалтера: аутсорсинг, ризики, захист інформації: монографія / Л.В.Чижевська, І.М. Вигівська, А.П.Дикий, Л.С.Скакун. – Житомир: ЖДТУ, 2011. – 404 с.
18. Шевелев А.Е. Риски в бухгалтерском учете: учебное пособие / А.Е. Шевелев, Е.В. Шевелева. – [2-е изд.]. - М.: КНОРУС, 2011. - 304 с.
19. Соломанидина Т.О., Соломанидин В.Г. Кадровая безопасность компании. – М.: Издательство «Альфа-Пресс», 2011. – 688 с.

Наукове видання

ОРГАНІЗАЦІЙНО-ЕКОНОМІЧНИЙ МЕХАНІЗМ ПРОТИДІЇ ЗЛОЧИНАМ В ЕКОНОМІЧНІЙ СФЕРІ

Колективна монографія за редакцією
Докторів економічних наук, професорів
Черевка Олександра Володимировича,
Мігус Ірини Петрівни,
Гнилицької Лариси Володимирівни

Технічний редактор Чабаненко Ю.А.
Оригінал-макет підготовлено Горячківською І.В.

Підписано до друку «13» січня 2017 р.
Формат 60х87/16. Папір офсетний
Гарнітура Times New Roman
Друк різографічний. Ум. друк. арк. 20,8
Наклад 300 прим. Зам. № 625

Видавництво: «Маклаут»
Свідоцтво про внесення до Державного реєстру видавців
Серія ДК №3014 від 11.08.2007 р.
Україна, м. Черкаси, вул. О. Дашкевича, 39
Тел.. (0472) 45-99-84
E-mail: office@2upost.com

Друк: ПП Чабаненко Ю.А.
Україна, м. Черкаси, вул. О. Дашкевича, 39
Тел.. (0472) 45-99-84
E-mail: office@2upost.com