Бобир Н.В.,*студентка,*
Білик В.В., *к.е.н., доцент*
доцент кафедри менеджменту та економічної безпеки,
Черкаський національний університет імені Богдана Хмельницького

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА – ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ

В умовах економіки постіндустріального суспільства,інформація, що стосується усіх напрямків діяльності підприємства, стає найбільш цінним і дорогим ресурсом, а проблеми інформаційної безпеки–усе більш складнимиіпрактичнозначущими.Інформаційна безпекаєоднією із складових частинекономічноїбезпеки, якаформуємодельзахищеностіпідприємства[2, с. 329].

Пріоритетним напрямком у процесі формування та забезпечення інформаційної безпеки будь-якого підприємства є збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг. Цевимагаєконкретнихдій, спрямованих на захистінформації з обмеженим доступом. Як свідчитьвітчизняна і закордоннапреса, кількістьзлочиніввінформаційнійсфері не тільки не зменшується, але й маєдоситьстійкутенденцію росту.

Для того щоб створити ефективну систему інформаційної безпеки необхідно чітко визначити загрози для інформаціїз обмеженим доступом. Під загрозами інформації з обмеженим доступом прийнято розуміти потенційні або реально можливі дії стосовно інформаційних ресурсів, що призводять до неправомірного оволодіння інформацією.

Джерелами зовнішніх загроз є: несумлінні конкуренти; злочинні угруповання і формування; окремі особи та організації адміністративно-управлінського апарата.

Джерелами внутрішніх загроз можуть бути: адміністрація підприємства; персонал; технічні засоби забезпечення виробничої і трудової діяльності.

Фахівці встановлюють в середньому наступне співвідношення зовнішніх і внутрішніх загроз: 82% загроз створюються співробітниками фірми або за їх прямої або опосередкованої участі; 17% загроз виникає ззовні – зовнішні загрози; 1% загроз створюється випадковими особами.

Основними загрозами інформації є її розголошення, витік і несанкціонований доступ до їїджерел.

Розголошення комерційних таємниць, найбільш розповсюджена дія власника (джерела), що призводить до неправомірного оволодіння конфіденційною інформацією за мінімальних витратах зусиль з боку зловмисника. Для цього він користується в основному легальними шляхами і мінімальним набором технічнихзасобів.

Реалізується розголошення формальними і неформальними каналами поширення інформації.

До формальних каналів поширення інформації належать: ділові зустрічі, наради, переговори та інші форми спілкування; обмін офіційними діловими, науковими і технічними документами, засобами передачі офіційної інформації.

Неформальними каналами поширення інформації є: особисте спілкування; виставки, семінари, конференції, з'їзди, колоквіуми та інші масові заходи;засоби масової інформації.

Як правило, причиною розголошення конфіденційної інформації є: слабке знання (або незнання) вимог захисту конфіденційної інформації; помилковість дій персоналу через низьку виробничу кваліфікацію;відсутність системи контролю за оформленням документів, підготовкою виступів, реклами і публікацій; злісне, навмисне невиконання вимог захисту комерційної таємниці[1, с. 224-225].

Наведена нижче таблиця дає уявлення про фактори, що сприяють розголошенню комерційнихсекретів.

Таблиця 1

№	Фактори	%
1.	Зайвабалакучістьспівробітників	32
2.	Прагненняспівробітниківзароблятигроші будь-якими способами і за будь-якуціну	24
3.	Відсутність на фірміслужбибезпеки	14
4.	«Радянські» звички співробітників фірми ділитися один з одним (тобто традиційний обмін досвідом)	12
5.	Безконтрольневикористанняінформаційних систем	10
6.	Наявність передумов для виникнення серед співробітників конфліктних ситуацій: відсутність психологічної сумісності, випадковий підбір кадрів.	8

Витік інформації загалом можна розглядати як неправомірний вихід конфіденційної інформації за межі організації або кола осіб, яким ця інформація була довірена.

Витік інформації за своєю суттю завжди припускає протиправне (таємне або явне, усвідомлене або випадкове) оволодіння конфіденційною інформацією, незалежно від того, яким шляхом це досягається.

Причини витоку, як правило,полягають у недосконалості норм щодо збереження комерційних таємниць, порушенні цих норм, а також відступі від правил поводження з відповідними документами, технічними засобами, зразками продукції та іншими матеріалами, що містять конфіденційну інформацію.

Умови включають різні фактори і обставини, що складаються в процесі наукової, виробничої, рекламної, видавничої, звітної, інформаційної та іншої діяльності підприємства і створюють передумови для витоку комерційних секретів.

Таким чином, значна частина причин і умов, що створюють передумови і можливість неправомірного оволодіння конфіденційною інформацією, виникають через недбалість керівників підприємств та їхніх співробітників[2, с. 330].

Несанкціонований доступ можна визначити як сукупність прийомів і порядок дій з метою одержання охоронюваних даних протиправним шляхом. До таких способіввідносяться, ті що порушують норми закону (таємне спостереження, підкуп службовця конкуруючої фірми або особи, що займається її постачанням, підслуховування телефонних переговорів, крадіжки креслень, зразків, документів, шпигунство і вимагання). До інших способів несанкціонованого доступу до інформації, можна віднести ті, які не порушують норм закону, але знаходяться на межі такої ситуації.

Окремі показники співвідношення способ і внесанкціонованого доступу наведені в таблиці 2.

Таблиця 2

№	Спосіб несанкціонованого доступу	%
1.	Підкуп, шантаж, переманюванняслужбовців, впровадженняагентів	43
2.	Знімання інформації з каналів зв'язку	24
3.	Проникнення в ПЕОМ	18
4.	Крадіжкадокументів	10
5.	Підслуховуваннятелефоннихрозмов	5

Аналізнаведенихданихпоказує,щозначначастинадійреалізуються в кримінальнійпрактиці за допомогоювикористання тих абоіншихтехнічнихзасобів[1, с. 225-226].

Таким чином, захист інформаційних ресурсів підприємства є одним з ключових завдань в умовах підвищення рівня внутрішніх і зовнішніх загроз інформаційної безпеки, що можуть безпосередньо вплинути на його фінансову діяльність і стійкість на ринку.

Список використаних джерел:

1. Чистоклетов Н. Г. Інформаційна безпека підприємства: сучасні реалії і загрози / Н. Г. Чистоклетов// Наукові записки Львівськогоуніверситетубізнесу та права. – 2015. – № 7. – с. 222-227.

2. Шевченко С. Ю. Формування системи управління інформаційної безпеки підприємства / С. Ю. Шевченко // КНЕУ імені Вадима Гетьмана. – 2012. – № 4. – с. 329-331.

Джалладова І.А., *д.фіз.-мат.н., професор,*
Бабинюк О.І., *к.е.н.,*
ДВНЗ «КНЕУ імені Вадима Гетьмана»

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ ЗАГРОЗ ЕЛЕМЕНТІВ КІБЕРПРОСТОРУ З ВИКОРИСТАННЯМ ДИФЕРЕНЦІАЛЬНИХ РІВНЯНЬ ІЗ ЗАПІЗНЕННЯМ

Актуальною проблемою сучасності є збереження інформаційних ресурсів від несанкціонованого доступу до елементів кіберпростору та порушення нормального функціонування інформаційних та телекомунікаційних систем. Кількість таких фактично злочинів зростає з кожним днем (рис. 1). Отже, виникає необхідність дослідження і розробки методів і моделей для аналізу ефективності систем захисту інформації [1].