Хоча деякі можуть подумати, що VMI збільшує ймовірність того, що помилки відбуватимуться з боку продавців, насправді VMI є набагато більше, ніж перенесення відповідальності та часу обробки. VMI допомагає зменшити загальний обсяг запасів у системі та зменшити обсяг обробки кожного окремого компонента, по суті, розширюючи фабрику або склад постачальника у власний виробничий центр. Постачальник розміщує інвентаризацію безпосередньо у виробничих осередках або інших областях використання, виключаючи необхідність отримання, обробки, підрахунку та переміщення компонентів від прийому до місця їх зберігання, а потім пункту використання.

Крім того, створення стандартних процедур по можливості може допомогти зменшити помилки. Підвищене повторення означає більш просту підготовку оператора і підвищене знайомство з процесом. Спрощена експлуатація має додаткову перевагу, що полегшує навчання працівників у різних частинах виробничого процесу. Крос-навчені працівники допомагають підвищити гнучкість робочої сили та ефективність.

Отже, стільникове виробництво стає трендом в бізнес-організаціях, тому що спрощує операції, є одним з найбільш ефективних і забезпечує відмінні позитивні результати.

Список використаних джерел та літератури:

1. Johns Ch. Improving Manufacturing Processes Through Lean Implementation [Електронний ресурс] – Режим доступу: https://www.qualitydigest.com/inside/ quality-insider-article/tips-improving-manufacturing-practices-through-lean-implementation

Науковий керівник: старший викладач кафедри менеджменту та економічної безпеки, к.е.н. Чередниченко В.В.

А. А. Северинчук
Черкаський національний університет імені Богдана Хмельницького

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА ЯК СКЛАДОВА ЕФЕКТИВНОГО ФУНКЦІОНУВАННЯ

Останніми десятиліттями спостерігається інтенсивний розвиток процесу інформатизації суспільства, що призвело до виникнення глобальної проблеми – інформаційної безпеки як підприємств України, так і суспільства у цілому. Діяльність підприємства залежить від стану навколишнього (зовнішнього та внутрішнього) інформаційного середовища. Будь-які впливи джерел інформаційного середовища на інформаційну сферу підприємства становлять загрозу і ризики для безпеки підприємства.

Інформаційна безпека підприємства є однією з головних для ефективного функціонування. У зв'язку з наявністю різноманітних способів конкурентного впливу з використанням інформації питання інформаційної безпеки набуває все більшої актуальності. Дослідженню інформаційної складової безпеки підприємство присвятили праці такі зарубіжні і вітчизняні вчені: Д. Граф, Н. МакДональд, К. Рассел, К. Скрипкін, В. Дудикевич, М. Карпінський та ін.

Питання інформаційної безпеки відображене у Законах України: «Про основи національної безпеки України» [1], «Про концепцію національної програми інформатизації» [2], «Про національну програму інформатизації» [3].

Поняття інформаційної безпеки підприємства полягає у формуванні принципів, методів та заходів щодо виявлення, аналізу, запобігання та нейтралізації негативних джерел, причин і умов впливу на інформацію. Крім того, дане поняття характеризує стан інформаційного захисту підприємства в умовах, з імовірністю загроз, що досягається системою заходів, спрямованих на попередження, виявлення та ліквідацію інформаційних загроз [4, с.139].

Виділяють дві групи загроз відносно інформаційної безпеки підприємства:

1. Ненавмисні, або випадкові дії (помилки в управлінні, неадекватна підтримка механізмів захисту тощо);

2. Навмисні дії (загрози) характеризуються несанкціонованим доступом до інформації і несанкціонованою маніпуляцією даними, ресурсами і самими системами.

Також, в окрему групу виділяють загрози, які пов'язані з навмисними помилками, що виникають у зовнішньому середовищі підприємства:

−розробка і поширення комп'ютерних вірусів різного характеру;

−перехоплення інформаційного потоку;

−несанкціонований доступ до інформації системи;

−зміна комп'ютерної інформації і підробка електронних підписів тощо [5].

Інформаційні технології знаходяться у стадії активного розвитку і це дає все більше можливостей доступу до інформаційних ресурсів та переміщення необхідних обсягів інформації на будь-яку відстань. З цієї причини підприємствам необхідно постійно посилювати та удосконалювати систему захисту доступу до інформації. Але при цьому виникає три проблеми.

Перша пов'язана з тим, що керівництво підприємства не завжди розуміє доцільність та необхідність посилення системи захисту інформаційної безпеки підприємства.

Друга полягає у відсутності достатньої кількості коштів. Відсутність фінансування для створення інформаційної безпеки підприємства зустрічається дедалі частіше.

Третя ж проблема є найнебезпечнішою. У цій ситуації керівництво підприємства визнає необхідність створення чи посилення системи інформаційної системи, виділяє на це кошти, але доручає цим займатись фахівцям без належної освіти та досвіду. Це може призвести до витоку інформації, надання доступу третім, зацікавленим особами, кібератакам тощо.

Розробка системи захисту інформаційної безпеки підприємства повинна ґрунтуватись на сучасних методах, що забезпечують максимальних захист від витоку інформації. До таких методів можна віднести: перешкоду, маскування, регламентацію, управління, примус і спонукання [6, с.159].

Окрім методів з метою запобігання витоку та втрати цінної інформації підприємствам доцільно використовувати 6 основних засобів:

−фізичні;

−апаратні;

−програмні;

−апаратно-програмні;

−законодавчі;

−криптографічні та організаційні методи.

Без належного захисту інформаційної безпеки підприємства ризикують своєю економічною безпекою.

На нашу думку, займатися розробкою та вдосконаленням системи інформаційної безпеки підприємства слід спеціальному підрозділу інформаційної безпеки, що входить до складу служби економічної безпеки підприємства. Саме в такому разі з'являються найкращі можливості вирішення проблем та питань інформаційної безпеки підприємства.

Отже, у сучасних умовах здійснення підприємницької діяльності інформаційна безпека є невід'ємною складовою системи економічної безпеки кожного підприємства. Розробка надійної системи захисту інформаційної безпеки забезпечує підприємству стійке положення та мінімізацію загроз інформації.

Список використаних джерел та літератури:

1. Про основи національної безпеки України: Закон України від 19 червня 2003 року № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

2. Про концепцію національної програми інформатизації: Закон України від 4 лютого 1998 року № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27-28. –Ст. 182.

3. Про національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27-28. – Ст. 181.

4. Нехай В. А., Нехай В. В. Інформаційна безпека як складова економічної безпеки підприємств./ В.А. Нехай, В.В. Нехай.// Науковий вісник Міжнародного гуманітарного університету : зб. наук. пр.- Одеса. Серія Економіка і менеджмент. – 2017. – №24(2). - С.137-140.

5. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби [Підручник] / В.Л. Бурячок, Г.М Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
6. Северина С. В. Інформаційна безпека та методи захисту інформації / С. В. Северина. // Вісник Запорізького національного університету. – 2016. – №1. – С. 155–160.

Науковий керівник: доцент кафедри менеджменту та економічної безпеки, к.е.н. Кравченко О.О.

А. А. Северинчук
Черкаський національний університет імені Богдана Хмельницького

ПОНЯТТЯ ТА ЗНАЧЕННЯ СТРАТЕГІЧНОГО ПЛАНУВАННЯ НА ПІДПРИЄМСТВІ

У діяльності українських підприємств важливе значення має розробка стратегічного планування з метою визначення цілей підприємства, а також обгрунтування шляхів досягнення поставлених цілей. Стратегічне планування необхідне країнам з невеликою економікою, до яких належить і Україна. Крім того, стратегічне планування відбувається під впливом нестабільного зовнішнього та внутрішнього середовища підприємства.

Питання необхідності розробки стратегічного планування для підприємств в сучасних умовах все ще актуальне.

Значний внесок у розв'язок даної проблеми зробили як вітчизняні, так і зарубіжні вчені: В.А. Винокуров, О.С.Віханський, В.Г. Герасимчук, М.І.Круглов, П.В. Забєлін, А.І. Ільїн, Д. Акер, І. Ансофф, У. Кінг, Д. Кліланд тощо.

Провідний український вчений Чучмарьова С. Ю. дає наступне визначення стратегічному плануванню: «Це основа стратегічного менеджменту, яка становить процес вибору цілей діяльності підприємства та шляхів їх досягнення, орієнтованих на потреби й запити споживачів, що забезпечує необхідні стратегічні зміни на підприємстві, адекватні змінам, що відбуваються в зовнішньому середовищі» [1, с.244].

Під час здійснення стратегічного планування основний акцент повинен робитися на розробку стратегічного плану. Також крім його розробки необхідною складовою є опрацювання заходів стосовно впровадження стратегічного плану в дію.

Єфремов В. С. в свою чергу визначає стратегічне планування як логічну послідовність декількох етапів, що включають сукупність процедур. За своїм характером їх можна об'єднати у дві групи: стратегічний аналіз і стратегічне проектування. До стратегічного аналізу належать: аналіз зовнішнього середовища, SWOT-аналіз. До стратегічного проектування відносять: розробка місії, дослідження стратегічного положення, формулювання цілей підприємства, планування реалізації стратегії [2,с.58].

Стратегічне планування має на меті оцінку перспектив, виявлення можливостей і загроз зовнішнього середовища, сильні та слабкі сторони внутрішнього середовища. Крім того, він допомагає аналізувати зміни конкурентоспроможності підприємства на ринку.

Розробка стратегічного плану забезпечує виживання підприємства в постійно змінних умовах, передбачає розвиток тих напрямів діяльності підприємства, що підвищують конкурентоспроможність на ринку.

Процес стратегічного планування проходить через 3 основних етапи.

І етап. Формується стратегія. Після цього визначається мета економічної діяльності підприємства, проводиться зовнішній та внутрішній аналіз.

ІІ етап. Стратегія набуває певної форми. Тобто підтвердження того, що стратегія буде реалізована у відповідній формі (програма, план, бюджет).

ІІІ етап. Оцінюється і контролюється впровадження стратегії. Порівнюються планові та звітні показники діяльності підприємства [3, с.466].

В процесі стратегічного планування центральне місце належить формуванню стратегічного набору підприємства, до складу якого входить перелік стратегій, тобто це прийняті керівництвом напрями і способи діяльності для досягнення довгострокових цілей