**УДК 338.242.2.**

# УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЇ В КОНТЕКСТІ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Студ. О.Ю.Галаган, гр. МгФБ-1-16
Науковий керівник проф. І.О. Тарасенко
Київський національний університет технологій та дизайну

***Метою*** наукового дослідження є розробка моделі системи захисту інформації, інтегрованої у систему управління фінансово-економічною безпекою підприємства.

Для досягнення цієї мети використано світовий досвід інформаційної безпеки приватних підприємств, існуючі моделі побудови системи інформаційної безпеки за міжнародними стандартами та управління ними.

***Об'єктом дослідження*** є процесс управління захистом інформації, його правові, фінансові, економічні та інформаційні особливості.

При проведенні наукового дослідження, по-перше, було використано відкриті дані моніторингу інформаційних небезпек в світі, приклади типових порушень інформаційної безпеки приватних підприємств та глобальні кібер-загрози, що дозволило власникам приватних підприємств з'ясувати основні проблеми і небезпеки та ймовірність їх виникнення у майбутньому. По-друге, з використанням структурного аналізу існуючих систем управління загальною фінансово-економічною безпекою приватних та державних підприємств визначено місце в ній системи захисту інформації.

Вперше було проведено аналіз усіх існуючих систем управління захистом інформації на прикладі найуспішніших компаній, які працюють в найбільш небезпечній з точки зору інформаційної безпеки індустрії – індустрії інформаційних технологій; зроблено аналіз компаній, які пропонують послуги з інформаційної безпеки.

Інформаційна безпеки включає три компоненти: вимоги, політику і механізми. Вимоги визначають цілі безпеки. Вони відповідають на питання - «Що ви очікуєте від вашої безпеки?». Політика визначає значення безпеки. Вона відповідає на питання - «Які кроки ви повинні зробити в досягненні цілей поставлених вище?». Механізми зумовлюють політику. Вони відповідають на питання - «Які інструменти, процедури та інші засоби ви використовуєте, щоб гарантувати те, що кроки зумовлені вище будуть виконані?» [1].

Багато підприємств-лідерів та індустріальні сектори бачать управління ризиками як новий підхід до управління інформаційною безпекою. Управління ризиками повинно допомогти їм у кількісному визначенні ймовірності небезпеки, оцінити ступінь можливих збитків і зважити витрати на безпеку проти їх очікуваної ефективності [2].

Управління ризиками має дати відповідь на наступні питання:

1. На скільки покращилася безпека підприємства в поточному році?
2. Що підприємство отримало за гроші, витрачені на безпеку?
3. На який рівень безпеки підприємство має орієнтуватися?

Для відповіді на ці питання потрібно суворе визначення параметрів безпеки і структури управління ризиками.

Можна виділити чотири найбільш важливі моменти в управлінні ризиками підприємства:

1. Недовговічність інформаційного активу. Підприємства і більшість промислових галузей розуміють, що ефективність їх роботи залежить від інформації.

Кожен відомий випадок критичного спотворення, пошкодження або руйнування інформації підсилює їх побоювання з цього пункту.

2. Доказова безпека. Оскільки параметри безпеки не завжди мають оцінку, підприємства не здатні виміряти стабільність або ефективність при виборі різних засобів забезпечення безпеки. Отже, кількість коштів, яке можна витратити на поліпшення безпеки не відомо.

3. Обгрунтування вартості. Підвищення вартості рішень і засобів безпеки призводить до того, що проекти інформаційної безпеки конкурують з іншими інфраструктурними проектами підприємства. Прибутково-вартісний аналіз і розрахунок ефективності використаних інвестиційних ресурсів стають стандартними вимогами для будь-яких проектів з інформаційної безпеки.

4. Відповідальність. Зі зростанням підприємств їх залежність від ризиків інформаційної безпеки зростає. Необхідний надійний механізм для управління цими ризиками. Для оцінювання інформаційної безпеки прибутково-вартісного аналізу і розрахунку коштів, які повертаються в результаті інвестицій, - недостатньо інформації. До цих пір немає методу, який дозволяє найбільш достовірно статистично представити параметри інформаційної безпеки [3].

Кожне підприємство повинно вибирати свій власний рівень достатності інформаційної безпеки. І на цьому тлі проводити збір даних для подальшого оцінювання. Оскільки реальні загрози майже завжди існують всередині підприємства, то достатній рівень безпеки зазвичай визначається тим, хто контролює внутрішні інформаційні показники.

З ускладненням інформаційних технологій підприємства стикаються все з більш складними інформаційними ризиками. Багато підприємств тонуть в потоці даних. У більшості випадків, наявна кількість фактів, дозволяє отримувати необхідну інформацію з оцінювання інформаційної безпеки. Але проблема в тому, що не завжди і не всі можуть отримувати цю інформацію. Для вирішенням цього завдання потребується розробка механізму, який дозволить аналізувати факти і, виділяючи необхідну інформацію, оцінювати її, перетворюючи в знання про безпеку.

ЛІТЕРАТУРА**:**

1. Bishop M. What Is Computer Security? / IEEE Security & Privacy Vol. 1, No. 1; January/February 2003, pp. 67-69.
2. Boehm B., Turner R. Using Risk to Balance Agile and Plan-Driven Methods / IEEE Computer Vol. 36, No. 6; June 2003, pp. 57-66.
3. Geer D. Risk Management Is Still Where the Money Is / IEEE Computer Vol. 36, No. 12; December 2003, pp. 129-131.