Підсекція «Управління фінансово-економічною безпекою»

УДК 331.1

ФОРМУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Студ. В.В. Асташов, гр. МгФБ-1-16
Науковий керівник доц. Н.В. Цимбаленко
Київський національний університет технологій та дизайну

Мета і завдання. Метою данного дослідження є обгрунтування пріоритету створення та управління системою інформаційної безпеки в контексті забезпечення економічної безпеки підприємства.

Завдання — аналіз систем інформаційної безпеки, оптимізація та покращення вже створених систем або формування ефективно діючих нових систем інформаційної безпеки.

Об'єкт дослідження. Об'єктом дослідження виступає система інформаційної безпеки суб'єкта господарювання.

Методи та засоби дослідження. З огляду на мету та завдання дослідження було обрано такі основні методи: аналіз та синтез.

Наукова новизна та практичне значення отриманих результатів. В сучасних умовах, питання щодо формування ефективної системи інформаційної безпеки суб'єктів господарювання є дуже актуальним і має важливе практичне значення з огляду на посилення дії загроз інформаційній безпеці підприємства.

Результати дослідження. На сьогоднішній день питання щодо формування ефективної системи інформаційної безпеки суб'єкта господарювання є дуже актуальним. Менеджмент підприємства має чітко розуміти цінність інформації, яка використовується в процесі економічної діяльності, та подбати про відповідний рівень її захисту.

Саме інформація стає об'єктом посягань з боку конкурентів підприємства. Варто зазначити, що конкуренти зазвичай використовують методи промислового шпіонажу, тобто намагаються заволодіти тією інформацією, яка є публічно не доступною і закритою. Саме ця інформація являє собою найбільшу цінність, оскільки вона містить відомості про канали збуту продукції, фінансову інформацію підприємства, постачальників, а також технології, які задіюються у виробничому процесі. Саме цей фактор має змусити менеджмент підприємства приймати відповідні міри захисту своїх даних. Підприємство має постійно покращувати роботу свого відділу безпеки якщо такий уже створений, або створити його, якщо до цього такого відділу не існувало. Захист виробничої та комерційної таємниці має вийти на перший план, оскільки успішний захист власних даних є однією з головних запорук конкурентоспроможності підприємства.[1]

Система управління інформаційною безпекою - це «частина загальної системи управління організації, що заснована на оцінці бізнес ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід та вдосконалення інформаційної безпеки». Серед основних її цілей можна виділити:

- забезпечення безпеки найважливішої корпоративної інформації;
- захист основних активів і бізнес-процесів підприємства;
- мінімізація ризиків інформаційної безпеки при веденні операційної діяльності підприємства;
- забезпечення безперервності основної діяльності підприємства;
- підвищення загального рівня управління підприємства.

Інформаційна безпека підприємства на практиці включає сукупність напрямів, методів, засобів і заходів, що знижують вразливість інформації та перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку. Елементами цієї системи є: правовий, організаційний, інженерно-технічний захист інформації; а основною її характеристикою - комплексність. Структура системи, склад і зміст елементів, їх взаємозв'язок залежать від об'єму і цінності інформації, що захищається, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи.[2]

Слід зазначити, що ключовим фактором, у забезпеченні інформаційної безпеки підприємства є його персонал. Основними заходами при роботі з яким є: проведення аналітичних процедур при прийомі і звільненні; навчання та інструктаж практичним діям по захисту інформації; контроль за виконанням вимог по захисту інформації, стимулювання відповідального відношення до збереження інформації та ін.

Не менш важливим є питання економічного обгрунтування витрат на захист інформації. Адже, чим вищий рівень захищеності інформації, тим, за інших рівних умов буде нижче розмір можливих збитків, але тим вищою буде вартість захисту. Оптимальний розміром витрат на захист буде такий, при якому забезпечується рівень захищеності, що дорівнює мінімуму загальних витрат.

Створити на підприємстві потужну систему інформаційної безпеки можливо двома способами. Перший спосіб полягає у наймі кваліфікованих фахівців та експертів, які допоможуть створити відповідну систему на підприємстві, другий спосіб полягає у створенні системи інформаційного забезпечення менеджерами підприємства без допомоги відповідних фахівців. Обидва способи мають свої переваги та недоліки. Переваги першого способу полягають у тому, що система інформаційного забезпечення створюється швидше, але окрім найму на відповідні посади працівників служби безпеки потрібно враховувати витрати на оплату праці фахівців, які дають відповідні підказки та рекомендації. Цей спосіб більш затратний, але швидший для реалізації в часі. Переваги другого способу полягають в тому, що він менш затратний, але в свою чергу вимагає більше часу для реалізації, через необхідність підвищення кваліфікації управлінського персоналу підприємства, з метою об’єктивного підбору працівників відділу інформаційної безпеки та навчання їх основам ефективного захисту цінної інформації.[3]

Отже, 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. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможними, підприємствам необхідно створити ефективну систему управління інформаційною безпекою. Сутність викладеного дає підстави стверджувати, що в сучасних умовах без належного захисту інформаційного середовища підпрієсмтва не можливо забезпечити його економічну безпеку.

ЛІТЕРАТУРА

1. Донець Л.І., Ващенко Н.В. Економічна безпека підприємства: Навч. пос. - К.: Центр учбової літератури, 2008. - 240 с.
2. Литвинюк А.А. Основи інформаційної безпеки. Комплексна система захисту інформації/ А.А. Литвинюк. – [Електронний ресурс]. – Режим доступу: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf.
3. Гриджук Г.С. Систематизація методів інофрмаційної безпеки підприємства / Гриджук Г.С. [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/natural/.