УДК 004.056.5

ФОРМУВАННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Студ. І.О. Щеглов, гр.Мг-УФЕБ-15
Наук. керівник доц. Ю.О. Русіна
Київський національний університет технологій та дизайну

В умовах економіки постіндустріального суспільства, інформація, що стосується усіх напрямків діяльності підприємства, стає найбільш цінним і дорогим ресурсом, а проблеми інформаційної безпеки – усе більш складними і практично значущими. Інформаційна безпека є однією із складових частин економічної безпеки, яка формує модель захищеності підприємства.

Різнобічному дослідженню питання забезпечення інформаційної безпеки присвячено праці С. Арзуманова, В. Домарєва, Є. Степанова, С. Петренка, О.Юдіна та ін.

Згідно з міжнародним стандартом ISO/IEC 17799:2005, 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 критичних бізнес-процесів організації; мінімізація ризиків інформаційної безпеки при веденні операційної діяльності організації; забезпечення безперервності основної діяльності організації; підвищення загального рівня управління організації.

Інформаційна безпека підприємства на практиці включає сукупність напрямів, методів, засобів і заходів, що знижують вразливість інформації і 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.

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 і 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 вище 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. Вартість збитків визначається двома параметрами: ймовірністю реалізації різних загроз інформації; важливістю інформації, захищеність якої може бути порушена під впливом різних загроз. У зв'язку зі складністю дати кількісну оцінку збитків причиною яких може бути витік, або втрата інформації, що захищається, в даний час найбільш доцільним є підхід на основі експертних оцінок. За даними висновків експертів можуть бути отримані статистично стійкі оцінки можливого збитку.

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 конкурентоспроможним, підприємствам необхідно створити ефективну систему управління інформаційною безпекою.