УДК 004.056.5

ФОРМУВАННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ

Студ. В.Ю. Острякова, гр. МгФБ-1-16
Науковий керівник доц. Ю.О. Русіна
Київський національний університет технологій та дизайну

Мета і завдання. Мета наукового дослідження – це обґрунтування пріоритету створення та управління системою інформаційної безпеки в контексті забезпечення економічної безпеки підприємства.

Завдання – це аналіз сутності системи управління інформаційною безпекою підприємств, проблем інформаційної безпеки, виявлення загроз в інформаційній безпеці, і як наслідок – визначення місця інформаційної безпеки в системі управління підприємством.

Об'єкт дослідження. Система управління інформаційною безпекою як підсистема загальної системи управління підприємством.

Методи та засоби дослідження. З огляду на мету і сформульоване завдання, а також об'єкт дослідження, використовувалися загальнонаукові та спеціальні методи пізнання: метод дедукції, індукції, емпіричний, комплексний та порівняння.

Наукова новизна та практичне значення отриманих результатів. Основні результати дослідження, що містять елементи наукової новизни, полягають у наступному:

- удосконалено систему забезпечення управління інформаційною безпекою підприємств;
- набули подальшого розвитку етапи побудови системи управління інформаційною безпекою підприємств.

Результати дослідження. В умовах сучасної економіки інформація стосовно всіх напрямків діяльності підприємства є найбільш цінним ресурсом, а проблеми інформаційної безпеки – усе складнішими і значущими. Інформаційна безпека є однією зі складових частин економічної безпеки, яка формує систему захищеності підприємства.

Дослідженню питання забезпечення інформаційної безпеки присвячені праці С. Арзуманова, С. Кавуна, І. Конєєва, Є. Степанова, С. Петренка, О. Юдіна та ін.

Згідно з міжнародним стандартом ISO/IEC 27001:2005, система управління інформаційною безпекою – це «частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розробки, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки». Її основними цілями є: конфіденційність інформації; неможливість несанкціонованого доступу до інформації; цілісність інформації, та пов'язаних з нею процесів; доступність інформації; мінімізація ризиків інформаційної безпеки шляхом виконання компенсаційних заходів; облік усіх процесів, пов'язаних з ризиками.

Суттєвими недоліками відповідно до забезпечення інформаційної безпеки підприємств є:

- відсутність паролів доступу в систему;
- відсутність паролів при роботі програмою з 1С: Підприємство, при зміні даних;
- відсутній додатковий захист файлів та інформації;
- нерегулярне оновлення баз програми антивіруса і сканування робочих станцій;

- велика кількість документів на паперових носіях, в основному, лежать в папках на робочому столі співробітника, що дозволяє зловмисникам скористатися даного роду інформацією у власних цілях;
- нерегулярне обговорення питань інформаційної безпеки на підприємстві і виникаючих проблем у цій галузі;
- нерегулярна перевірка працездатності інформаційних систем підприємства, налагодження проводиться лише в тому випадку, коли вони виходять з ладу;
- відсутня політика інформаційної безпеки;
- відсутність системного адміністратора.

Для нейтралізації існуючих загроз і забезпечення інформаційної безпеки підприємства організовують систему управління у сфері інформаційної безпеки, в рамках якої проводять роботу по декількох напрямах:

- формування і практична реалізація комплексної багаторівневої політики інформаційної безпеки підприємства і системи внутрішніх вимог, норм і правил;
- організація служби інформаційної безпеки;
- розробка системи заходів і дій на випадок виникнення непередбачених ситуацій;
- проведення аудитів стану інформаційної безпеки на підприємстві.

Основними етапами побудови системи управління інформаційної безпеки є наступні:

1) визначення сфери дії системи управління інформаційною безпекою (може охоплювати все підприємства, єдиний офіс або виділений сервіс);

2) створення набору внутрішніх нормативних документів (політик, процедур, корпоративних стандартів, інструкцій). Документована політика інформаційної безпеки повинна бути затверджена керівництвом і доведена до відома всіх співробітників організації і зовнішніх сторін, до яких вона відноситься;

3) вибір методу оцінки ризиків, прийнятний для організації й області дії системи управління інформаційної безпеки. Необхідно оцінити ризики, включаючи: вплив на цілісність, конфіденційність і доступність ресурсів; вірогідність настання ризиків; рівень ризиків;

4) ухвалення рішення про подальші дії відносно виявлених ризиків (можна прийняти ризики, відповідні допустимому рівню системи управління інформаційною безпекою, запропонувати механізми контролю для їх мінімізації, адресувати ризики третій стороні (наприклад, за допомогою страхування). Також можуть бути застосовані додаткові заходи контролю);

5) впровадження – ця частина циклу передбачає управління механізмами контролю, що передбачають перевірку досягнення мети, моніторинг загроз і недоліків та періодичні оцінки.

Висновки. Інформаційна безпека є однією з ключових частин формування системи захищеності підприємства. Для збереження підприємства, його розвитку та конкурентоспроможності необхідне створення ефективної системи управління інформаційною безпекою. Сутність викладеного вище дає підстави стверджувати, що в сучасних умовах без належного захисту інформаційного середовища, підприємствам неможливо забезпечити економічну безпеку.

Ключові слова. Інформаційна безпека, система управління інформаційною безпекою, недоліки інформаційної безпеки, етапи створення системи управління інформаційною безпекою.