Марунич А. В.

Магістр 1 року навчання
факультету обліку і аудиту ХНЕУ ім. С. Кузнеця

УДК 005.3:004

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В УПРАВЛІННІ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ

Анотація. Досліджено теоретичні засади та практичний інструментарій застосування сучасних інформаційних технологій в управлінні безпекою організації. Розглянуто напрями використання інформаційних технологій щодо оптимізації та запобігання загроз діяльності організації. Сформовано перелік функцій ефективної системи управління інформаційною безпекою.

Аннотация. Исследованы теоретические основы и практический инструментарий применения современных информационных технологий в управлении безопасностью организации. Рассмотрены направления использования информационных технологий по оптимизации и предотвращению угроз деятельности организации. Сформирован перечень функций эффективной системы управления информационной безопасностью.

Annotation. The theoretical basis and practical application of the modern tools of information technologies in the security management of organizations are studied. The use of information technologies aiming to prevent threats and optimize the organization activity is considered. A list of functions of the effective information security management system is offered.

Ключові слова: організація, безпека, управління, інформаційні технології, загрози, система управління інформаційною безпекою, інфокомунікаційні системи, політика безпеки.

Інформація є одним із головних ділових ресурсів, який забезпечує організації додану вартість, і внаслідок цього потребує захисту. Слабкі місця в захисті інформації можуть призвести до фінансових втрат і нанести збиток комерційним операціям. Тому в наш час питання розробки системи управління інформаційною безпекою та її впровадження в організації є концептуальним.

Нові інформаційні технології в управлінні безпекою є важливим і необхідним засобом, який дозволяє:

1) швидко, якісно та надійно виконувати отримання, облік, зберігання й обробку інформації;

2) значно скоротити управлінський персонал організації, який займається роботою зі збору, обліку, зберігання й обробки інформації;

3) забезпечити у потрібні терміни керівництво й управлінсько-технічний персонал організації якісною інформацією;

4) своєчасно та якісно вести аналіз і прогнозування господарської діяльності організації;

5) швидко та якісно приймати рішення з усіх питань управління організацією [1].

Теоретичні та практичні питання, пов'язані з дослідженням аспекту використання інформаційних технологій, були висвітлені в роботах як західних вчених: Т. Мейора, І. Стікула, А. Коберна, так і українських: М. Матвєєва, Ю. Петрова, Ю. Румнянцева, К. Красноперова, А. Матвієнка, Степаненко О. П., Чернявського А. Д.

Метою статті є розгляд тенденції приваблення іноземних інвестицій, що змушує комерційні організації впроваджувати міжнародні стандарти управління, в тому числі і стандарти управління інформаційною безпекою. Ці факти пояснюють підвищення попиту на впровадження систем управління інформаційною безпекою українських організацій.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1) розкрити сутність політики інформаційної безпеки;

2) визначити основні етапи розробки системи управління інформаційною безпекою;

3) сформулювати перелік функцій ефективної системи управління інформаційною безпекою.

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики. Загальне призначення СУІБ – розроблення, впровадження, функціонування, моніторинг, перегляд, підтримування та вдосконалення інформаційної безпеки (ІБ) [2].

Під політикою інформаційної безпеки слід розуміти набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації й спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано до підприємства, інформаційної системи, окремого персонального комп'ютера (ПК) тощо.

Політика інформаційної безпеки в інфокомунікаційній системі (ІКС) є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у галузі інформаційної безпеки. Для кожної ІКС політика безпеки інформації може бути індивідуальною і може залежати від використовуваної технології обробки інформації, особливостей операційної системи, фізичного середовища і від багатьох інших чинників. ІКС може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій ІКС буде складеною з частин, що відповідають різним технологіям та іншим особливостям. Очевидно, що для різних ІКС відповідні системи (політики) інформаційної безпеки можуть істотно відрізнятись.

Політика безпеки повинна визначати ресурси ІКС, що потребують захисту, зокрема установлювати категорії інформації, оброблюваної в ІКС. Як складові частини загальної політики інформаційної безпеки в ІКС мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації.

Що стосується основних етапів розробки СУІБ, то виділяють такі:

1) інвентаризація активів;

2) категорювання активів;

3) оцінка захищеності інформаційної системи;

4) оцінка інформаційних ризиків;

5) обробка інформаційних ризиків (у тому числі визначення конкретних заходів для захисту цінних активів);

6) упровадження вибраних заходів обробки ризиків;

7) контроль виконання та ефективність вибраних заходів;

8) роль керівництва організації в СУІБ [3].

Одним з основних умов ефективного функціонування СУІБ є залучення керівництва компанії в процес управління ІБ. Усі співробітники повинні розуміти, що, по-перше, вся діяльність із забезпечення ІБ ініційована керівництвом і обов'язкова для виконання, по-друге, керівництво організації особисто контролює функціонування СУІБ, по-третє, саме керівництво виконує ті ж правила.

Ураховуючи основні вимоги стосовно СУІБ, сформульовані необхідні функції програмного продукту для управління інформаційною безпекою:

1) представлення для керівників високого рівня завдяки простим інтерфейсам та звітам, орієнтованим на вище керівництво;

2) відстеження й управління ризиками ІБ на підприємстві з негайною переоцінкою в разі будь-яких змін у наборах активів чи загроз; планування зовнішнього або внутрішнього аудиту, контроль процесу аудиту за допомогою зведених звітів;

3) реєстрація порушень, відхилень та зауважень у процесі аудиту шляхом подання потрібної інформації в спеціальному звіті;

4) використання шаблонів для політик, описів та інших робочих документів (ці шаблони повинні відповідати державним стандартам України);

5) створення і зберігання всіх необхідних настановних та регулюючих документів ІБ (функціональні обов'язки, інструкції, політики безпеки тощо) шляхом зберігання, оновлення та включення інформації щодо ІБ в установі безпосередньо до документів;

6) підтримання спільних баз знань та методичних матеріалів, архівація для забезпечення управлінських рішень фактичними даними;

7) проведення аналізу стану ІБ і створення звітів для правління у вигляді зрозумілих таблиць і діаграм, оскільки представити інформацію щодо ІБ неспеціалістам зазвичай проблематично;

8) раціональний розподіл ролей, повноважень і ресурсів між співробітниками та завданнями;

9) інформативно-аналітична підтримка рішень правлінням організації відносно управління ІБ, тому що за наявності зрозумілої та об'єктивної інформації приймати раціональні рішення легше [2].

Отже, система управління інформаційною безпекою дає організації такі переваги, як: управління інформаційною безпекою організації в рамках єдиної корпоративної політики, управління ризиками та їх своєчасне виявлення, зниження ризиків від зовнішніх і внутрішніх загроз, систематизація процесів забезпечення інформаційною безпекою, встановлення пріоритетів організації у сфері інформаційної безпеки. У свою чергу, це забезпечує організації конкурентну перевагу, демонструючи здатність керувати інформаційними ризиками, при цьому також збільшується її капіталізація.

Наук. керівн. Москаленко Н. О.

Література: 1. Кастельс М. Информационная эпоха: экономика, общество и культура / М. Кастельс ; пер. с англ. под науч. ред. О. И. Шкаратана. – М. : ГУ ВШЭ, 2008. – С. 77–78. 2. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). ГСТУ СУИБ 1.0/ISO/IEC 27001:2010. – К. : Національний банк України, 2010. – 49 с. 3. ISO 27001:2005 "Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційною безпекою – Вимоги. – К. : Держстандарт, 2005. 4. Інформаційні технології. Методи захисту. Звіт правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD). ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – К. : Національний банк України, 2010. – 163 с. 5. Ярочкин В. И. Безопасность информационных систем / В. И. Ярочкин. – М. : Изд. "Ось-89", 2006. – 187 с.