УДК 004.056.5

Печенюк Андрій
к.е.н., доцент
Подільський державний аграрно-технічний університет
м. Кам'янець-Подільський

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУЧАСНОГО ПІДПРИЄМСТВА

Анотація

Проаналізовано джерела загроз інформаційній безпеці сучасного підприємства, наведено класифікацію основних видів загроз; узагальнено головні етапи побудови політики інформаційної безпеки; виділено підсистеми ефективного захисту інформації на підприємстві; розроблено рекомендації з проектування політики інформаційної безпеки.

***Ключові слова**: захист інформації, інформаційна система, інформаційна безпека, інформаційна технологія, антивірусний захист, політика інформаційної безпеки, конфіденційність інформації, цілісність інформації, криптографічний захист, несанкціонований доступ.*

На сьогоднішній день своєчасна та об'єктивна інформація є важливим фактором виробництва, який розглядають, як один з основних ресурсів розвитку суспільства. Сучасні інформаційні системи та технології є засобом підвищення продуктивності та ефективності роботи працівників.

Проте глобальна комп'ютеризація у багатьох сферах управління та виробництва супроводжується появою принципово нових загроз інтересам особистості, підприємства, суспільства, держави [4].

Паралельно з розвитком і ускладненням засобів, методів, форм автоматизації процесів обробки інформації підвищується залежність суб'єктів підприємництва від ступеню безпеки використовуваних ними інформаційних технологій [2].

Можна виділити цілу низку джерел загроз інформаційній безпеці сучасного підприємства:

– протизаконна діяльність деяких економічних структур у сфері формування, поширення і використання інформації;

– порушення встановлених регламентів збору, обробки та передачі інформації;

– навмисні дії та ненавмисні помилки персоналу інформаційних систем;

– помилки в проектуванні інформаційних систем;

– відмова технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах тощо [4].

На сьогоднішній день фахівцями досліджується досить широкий перелік загроз безпеці інформаційних систем [2], які класифікують за рядом ознак (рис. 1).

***Рис**. 1. Класифікація загроз безпеці інформаційної системи*

Захист інформації – галузь науки і техніки, яка динамічно розвивається, пропонує ринку широкий спектр засобів для захисту даних. Проте жоден з них окремо взятий не може гарантувати адекватну безпеку інформаційної системи. Необхідною умовою ефективного захисту є проведення комплексу взаємодоповнюючих заходів [1].

Комплексне забезпечення інформаційної безпеки автоматизованих систем – це сукупність криптографічних, програмно-апаратних, технічних, правових, організаційних методів і засобів забезпечення захисту інформації при її обробці, зберіганні та передачі з використанням сучасних комп'ютерних технологій [2].

З липня 2003 р. в Україні введена кримінальна відповідальність за незаконне втручання в роботу комп'ютерів і комп'ютерних мереж, а також за поширення комп'ютерних вірусів, що призвело до спотворення, зникнення, блокування інформації чи її носіїв [1].

Досвід показує, що практично кожне підприємство має антивірусні засоби захисту, системи ідентифікації користувачів, системи управління доступом до інформаційної системи тощо. Тобто потенціал засобів захисту є, але він не реалізується фірмами повністю. Більше того, володіючи складними апаратними засобами захисту інформації, більшість підприємств навіть наполовину не

використовують їх потенціал. Переважна більшість вимог стандартів інформаційної безпеки можуть бути реалізовані наявними у фірм засобами захисту [5].

Сучасне підприємство повинно вміти належним чином будувати політику інформаційної безпеки, тобто розробляти і ефективно впроваджувати комплекс превентивних заходів по захисту конфіденційних даних та інформаційних процесів. Така політика передбачає відповідні вимоги на адресу персоналу, менеджерів і технічних служб [2].

Головними етапами побудови політики інформаційної безпеки є:

1) реєстрація всіх ресурсів, які мають бути захищені;
2) аналіз та створення переліку можливих загроз для кожного ресурсу;
3) оцінка ймовірності появи кожної загрози;
4) вжиття заходів, які дозволяють економічно ефективно захистити інформаційну систему [1].

Більшість фахівців у галузі захисту інформації вважають, що інформаційна безпека підтримується на належному рівні, якщо для всіх інформаційних ресурсів системи підтримується відповідний рівень конфіденційності (неможливості несанкціонованого отримання будь-якої інформації), цілісності (неможливості навмисної або випадкової її модифікації) і доступності (можливості оперативно отримати запитувану інформацію) [2].

Можна виділити такі підсистеми ефективного захисту інформації на підприємстві:

1. Підсистема антивірусного захисту шлюзів входу в мережу Інтернет, файлових серверів, робочих місць користувачів, централізованого управління, періодичного оновлення антивірусних баз даних.
2. Підсистема управління контролем доступу та ідентифікацією в інформаційній системі.
3. Підсистема міжмережного екранування, яка дозволяє реалізувати безпеку міжмережної взаємодії через використання програмних і програмно-апаратних міжмережних екранів.
4. Підсистема криптографічного захисту, яка гарантує безпеку передачі інформації завдяки шифруванню даних.
5. Підсистема забезпечення цілісності інформації та програмного середовища шляхом застосування відповідних засобів для фіксації та контролю стану програмного комплексу, управління зберіганням даних для резервного копіювання та архівування.
6. Підсистема захисту від інсайдерів, яка контролює дії порушників, реалізує інформаційну безпеку при управлінні доступом і реєстрації.
7. Підсистема захисту систем управління базами даних.
8. Підсистема виявлення вторгнень і спроб несанкціонованого доступу до інформаційних ресурсів підприємства. Підсистема забезпечує реалізацію захисних заходів з протидії атакам хакерів і поширенню спаму.
9. Підсистема захисту мобільних пристроїв.
10. Підсистема моніторингу подій інформаційної безпеки, яка дозволяє своєчасно виявляти загрози інформаційній системі та оперативно реагувати на них [5].

Сьогодні спеціалізовані фірми пропонують широкий спектр засобів захисту інформаційних систем з урахуванням їх вартості та функціональних можливостей. Найбільш прийнятним підходом при виборі того чи іншого варіанту є дотримання принципу «розумної достатності», суть якого полягає в тому, що визначальними при проектуванні політики інформаційної безпеки повинні бути: розмір підприємства, його ресурсні та фінансові можливості, поточний рівень інформаційної безпеки, стадія функціонування фірми.

Постійна робота в сфері підтримки інформаційної безпеки на належному рівні є необхідною умовою ефективності підприємницької діяльності [5].

Водночас безпека інформаційної системи має розглядатися як важлива складова загальної безпеки підприємства. Причому необхідна розробка концепції інформаційної безпеки, в якій слід передбачити не тільки заходи, пов'язані з інформаційними технологіями (криптозахист, програмні засоби адміністрування прав користувачів, їх ідентифікації та автентифікації, брандмауери для захисту входів-виходів мережі тощо), але і відповідні заходи адміністративного та технічного характеру [3].

Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, обробки, зберігання, пошуку та надання користувачам. Ці технології мають враховувати особливості інформації, які роблять її цінною, а також давати змогу користувачам різних категорій ефективно працювати з інформаційними ресурсами.

Список використаних джерел

1. Батюк А.Є. Інформаційні системи в менеджменті / А.Є. Батюк, З.П. Двуліт, К.М. Обельовська, І.М. Огороднік, Л.П. Фабрі. – Львів: «Інтелект-Захід», 2004. – С. 343–384.

2. Власова Л.А. Защита информации / Л.А. Власова. – Хабаровск: РИЦ ХГАЭП, 2007. – 84 с.

3. Замкова Т.В. Проблемы защиты информации в современных информационных системах / Т.В. Замкова. – [Електронний ресурс]. – Режим доступу: http://www.rae.ru/snt/?section=content&op=show_article&article_id=3893

4. Литвинюк А.А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування // А.А. Литвинюк. – [Електронний ресурс]. – Режим доступу: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf

5. Матиев Д. Средства защиты информации: проблема выбора и соответствия / Джабраил Матиев. – Електронний ресурс. – Режим доступу: http://bankir.ru/publikacii/s/sredstva-zaschiti-informacii-problema-vibora-i-sootvetstviya-5386161/