Головним напрямом захисту документованої інформації від можливих небезпек є формування захищеного документообігу, тобто використання в обробці і зберіганні документів спеціалізованої технологічної системи, що забезпечує безпеку інформації на будь-якому типі носія.

Список використаної літератури

1. Храмцовская Н. А. Международные стандарты, информационная безопасность и управление документацией / Н. А. Храмцовская // Делопроизводство и документооборот на предприятии. – 2005. – № 3. – С. 30–36.

2. Дубов Д. В. Проблеми нормативно-правового забезпечення інформаційного суверенітету в Україні : аналітична записка [Електронний документ] / Д. В. Дубов. – Режим доступу: www.niss.gov.ua

3. Зибін С. В. Захист інформації від несанкціонованого доступу в системах обробки інформації / С. В. Зибін // Інформаційна безпека. – 2011. – № 1.

Щербіна О. С., канд. екон. наук,
Поліщук Н. Л.,
Донецький національний університет, м. Вінниця

ІНФОРМАЦІЙНІ РЕСУРСИ ЯК СКЛАДОВА БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

У сучасних умовах посилення тенденцій глобалізації й інформатизації суспільства роль інформації в усіх сферах життєдіяльності значно зростає. Інформація стає необхідною умовою й елементом будь-якої виробничої діяльності, що за своєю значимістю все більше прирівнюється до енергетичних і сировинних ресурсів і використовується для заміщення живої праці, сировини й енергії.

Лише останнім часом посеред ресурсів підприємства, які поділяються на матеріальні і трудові, почали виділяти інформаційні ресурси та детально аналізувати їхні склад, структуру, рівень використання та ін. [1].

Під інформаційними ресурсами підприємства розуміють сукупність нематеріальних активів, документів, що мають важливе стратегічне значення для функціонування організації [2].

Інформаційні ресурси мають ряд специфічних властивостей:

– не витрачається в процесі використання;
– розширення їхнього споживання практично не має обмеження;
– мають високу ресурсозберігаючу здатність.

Інформаційні ресурси підприємства служать інструментами стимулювання виробничо-комерційної діяльності, прийняття управлінських рішень і навчання [1].

Отже, актуальною темою сьогодення є забезпечення захисту інформаційних ресурсів підприємства від чужого вторгнення, адже безпека інформаційної системи підприємства є одним з основних факторів, що забезпечує ефективний документообіг, який, в свою чергу, є засобом підвищення продуктивності та ефективності роботи працівників та, як наслідок, забезпечення розвитку всього підприємства.

В українському законодавстві ще немає Державного стандарту, що визначає загальні положення захисту інформації і навіть джерела з системно викладеною термінологією в сфері інформатизації.

На практиці виділяють три базові принципи інформаційної безпеки:

–доступність інформації (можливість за розумний час отримати необхідну інформацію);

–цілісність (актуальність і несуперечливість інформації, її захищеність від руйнування та несанкціонованої зміни);

–конфіденційність (захист від несанкціонованого прочитання) [3].

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.

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.

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.

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.

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 їхній потенціал. Переважна більшість вимог стандартів інформаційної безпеки можуть бути реалізовані наявними у фірм засобами захисту.

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

Головними етапами побудови політики інформаційної безпеки є:

– реєстрація всіх ресурсів, які мають бути захищені;

– аналіз та створення переліку можливих загроз для кожного ресурсу;

– оцінка ймовірності появи кожної загрози;

– вживання заходів, які дозволяють економічно ефективно захистити інформаційну систему.

Більшість фахівців у галузі захисту інформації вважають, що інформаційна безпека підтримується на належному рівні, якщо на практиці для всіх інформаційних ресурсів системи підтримується відповідний рівень всіх трьох базових принципів інформаційної безпеки, що були розглянуті раніше.

Сьогодні спеціалізовані фірми пропонують широкий спектр засобів захисту інформаційних систем з урахуванням їхньої 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.

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, але і відповідні заходи адміністративного та технічного характеру.

Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їхнього власника. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їхнього 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 [4].

Список використаної літератури

1. Чернявська І. Інформаційні ресурси підприємства як джерело економічного зростання промислового підприємства [Електронний ресурс] / І. Чернявська. – Режим доступу: http://www.econa.at.ua/Vypusk_2/Chernyavska.pdf

2. Вяткін П. С. Елементи стратегічного управління інформаційними ресурсами сільськогосподарських підприємств [Електронний ресурс] / П. С. Вяткін. – Режим доступу: https://chdtu.edu.ua/files/feu/Pratsi/KEU/Viatkin/Stat_strat_inf.pdf

3. Сікорський Д. О. Аналіз термінології в українському законодавстві, що регламентує діяльність в сфері інформатизації / Д. О. Сікорський // Інвестиції: практика та досвід. – К. : ТОВ «ДКС Центр». – 2014. – № 7. – С. 125–128.

4. Печенюк А. Особливості організації інформаційної безпеки сучасного підприємства [Електронний ресурс] / А. Печенюк. – Режим доступу: http://sophus.at.ua/publ/2014_04_17_18_kampodilsk/sekcija_4_2014_04_17_18/osoblivosti_organizaciji_informacijnoji_bezpeki_suchasnogo_pidpriemstva/54-1-0-931