РОЗДІЛ 2. Проблеми та перспективи функціонування підприємства і підприємництва

УДК 338.2:346.2

Бєляєва Л.А.,
к.е.н., доцент кафедри економіки та фінансів
Харківського національного університету внутрішніх справ,
м. Харків

СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Розкриті проблеми забезпечення інформаційної безпеки при використанні комп'ютерних систем і комунікаційних мереж та запропоновані заходи щодо запобігання погроз інформаційної безпеки та усуненню їх наслідків.

Ключові слова: *інформаційна безпека, комп'ютерні системи, погрози інформаційної безпеки, заходи безпеки: правові, кадрові, організаційні, апаратні, програмні, криптографічні.*

Постановка проблеми. Проблема забезпечення інформаційної безпеки актуальна для держави, підприємств і організацій усіх форм власності, які останнім часом приділяють повсякденну увагу інформаційній безпеці, залучаючи для її рішення фахівців власних служб безпеки й оснащені сучасною технікою спеціалізовані структурні підрозділи.

Актуальність проблеми захисту інформації сьогодні не викликає сумнівів. Успіх сучасного підприємництва і його розвиток в умовах гострої конкуренції в значній мірі залежать від застосування інформаційних технологій, а отже, від ступеня забезпечення інформаційної безпеки.

Актуальність дослідження полягає також і в тому, що розвиток глобальної мережі Інтернет і супутніх технологій досяг такого високого рівня, що сьогодні діяльність будь-якого підприємства в цілому й кожного користувача окремо неможливо уявити без електронної пошти, спілкування в режимі «он-лайн» та Web-реклами.

Поширення комп'ютерних систем і об'єднання їх у комунікаційні мережі підсилює можливості електронного проникнення до них. У всіх країнах світу існує проблема комп'ютерної злочинності, що викликає необхідність залучення все більшої уваги й сил для організації боротьби з даним видом злочинів.

Будь-яке підприємство має у своєму розпорядженні різні види інформації, що уявляють інтерес для зловмисників. Насамперед, це комерційні й конфіденційні дані, інформація, що є інтелектуальною власністю підприємства.

Аналіз останніх досліджень та публікацій. Інформаційна безпека – досить ємна й багатогранна проблема, що охоплює не тільки визначення необхідності захисту інформації, але й те, як її захищати, від чого захищати, коли захищати, чим захищати і яким повинен бути цей захист.

Аналіз робіт вчених і фахівців-практиків дозволяє виділити наступні найбільш гострі проблеми розвитку теорії й практики інформаційної безпеки:

- створення теоретичних основ і формування науково-методологічного базису, що дозволять адекватно описувати процеси в умовах інформаційних погроз;

- розробка науково-обґрунтованих нормативно-методичних документів, щодо забезпечення інформаційної безпеки на базі дослідження й класифікації погроз інформації та розробка стандартів-вимог до її захисту;
- стандартизація підходів до створення систем захисту інформації й раціоналізація схем і структур управління захистом на підприємствах безпосередньо і в цілому на державному рівні.

Метою дослідження є визначення основних напрямків системи захисту інформації і визначення комплексу заходів, щодо запобігання погроз інформаційної безпеки за різними напрямами, безпосередньо в практиці діяльності підприємств та організацій.

Виклад основного матеріалу. На сьогодні відбувається швидкий розвиток засобів обчислювальної техніки й мереж передачі даних, що дозволяє на основі оперативного обміну інформацією створювати нові напрямки в науці, банківській, управлінській та підприємницькій діяльності. Проникнення комп'ютерних технологій в усі сфери людського життя привело до необхідності розробки надійних способів рішення проблеми захисту інформації, що циркулює в комп'ютерних системах, від несанкціонованого доступу.

У забезпеченні інформаційної безпеки потребують різні суб'єкти інформаційних відносин, такі як: держава в цілому, суспільні або комерційні підприємства; окремі громадяни (фізичні особи).

Існує безліч визначень захисту інформації через широту поняття «інформація» і багатозначності поняття «інформаційна безпека».

Так, під захистом інформації у вузькому значенні розуміють сукупність заходів і дій, спрямованих на забезпечення її безпеки: конфіденційності й цілісності – у процесі збору, передачі, обробки й зберігання, а в більш широкому значенні розуміють комплекс організаційних, правових і технічних заходів щодо запобігання погроз інформаційної безпеки та усуненню їх наслідків.

Сутність захисту інформації полягає у виявленні, усуненні або нейтралізації негативних джерел, причин і умов впливу на інформацію. Захист інформації спрямований:

- на попередження погроз як превентивних заходів щодо забезпечення інформаційної безпеки в інтересах попередження можливості їх виникнення;
- на виявлення погроз, яке виражається в систематичному аналізі та контролі можливості появи реальних або потенційних погроз і своєчасних заходах для їх попередження;
- на локалізацію злочинних дій і вживання заходів по ліквідації погроз або конкретних злочинних дій;
- на ліквідацію наслідків погроз і злочинних дій і відновлення інформації.

При аналізі проблем, пов'язаних з інформаційною безпекою, необхідно враховувати специфіку даного аспекту безпеки, яка полягає в тому, що інформаційна безпека є складовою частиною інформаційних технологій – галузі, яка розвивається безпрецедентно високими темпами. Тут важливі не стільки окремі рішення (закони, програмно-технічне забезпечення), що перебувають на сучасному рівні, скільки механізми генерації нових ідей, що дозволяють жити в темпі технічного прогресу. Одним з найважливіших аспектів проблеми для забезпечення інформаційної безпеки є визначення, аналіз і класифікація можливих погроз безпеки інформації.

Під загрозою безпеки розуміється потенційно можлива подія, процес або явище, які можуть привести до знищення, втрати цілісності, конфіденційності або доступності інформації.

Всю безліч погроз можна розділити на два класи: випадкові або навмисні (рис.1).

Погрози, які не пов'язані з навмисними діями злочинців і реалізуються випадково, називають випадковим або ненавмисними. Реалізація погроз цього класу приводить до найбільших втрат інформації, при цьому може відбуватися знищення, порушення цілісності й доступності інформації. Рідше порушується конфіденційність інформації, але при цьому створюються передумови для злочинного впливу на інформацію.

Стихійні лиха й аварії можуть призводити до найбільших фізичних руйнівних наслідків для матеріальних джерел зберігання інформації, тому що вона втрачається або доступ до неї стає неможливий.

Збої й відмови складних систем неминучі. У результаті порушується працездатність технічних засобів, знищуються й спотворюються дані і програми. Порушення роботи окремих вузлів і обладнань можуть також привести до порушення конфіденційності інформації, до несанкціонованого доступу до інформації шляхом несанкціонованої її видачі в канал зв'язку, на друкувальний пристрій.

Рис. 1. Погрози інформаційної безпеки у комп'ютерних системах

Алгоритмічні й програмні помилки, при розробці інформаційної системи, приводять до наслідків, аналогічних наслідкам збоїв і відмов технічних засобів. Крім того, такі помилки можуть бути використані зловмисниками для впливу на ресурси

інформаційної системи. Особливу небезпеку становлять помилки в операційних системах і в програмних засобах захисту інформації.

Найбільший відсоток випадків порушення безпеки інформації відбувається в результаті помилок користувачів і обслуговуючого персоналу. Некомпетентне, недбале або неуважне виконання функціональних обов'язків співробітниками приводять до знищення, порушення цілісності й конфіденційності інформації, а також компрометації механізмів захисту.

Характеризуючи погрози інформації, не пов'язані з навмисними діями, у цілому, слід зазначити, що механізм їх реалізації вивчений досить добре, накопичений значний досвід протидії цим погрозам. Сучасна технологія розробки технічних і програмних засобів, ефективна система експлуатації інформаційних систем, що включає обов'язкове резервування інформації, дозволяють значно знизити втрати від реалізації погроз цього класу.

Клас навмисно створюваних погроз вивчений недостатньо, дуже динамічний і постійно поповнюється новими формами.

До методів шпигунства й диверсій відносять: підслуховування; візуальне спостереження; розкрадання документів і машинних носіїв інформації; розкрадання програм і атрибутів системи захисту; підкуп і шантаж співробітників; збір і аналіз відходів машинних носіїв інформації; підпали; вибухи.

Несанкціонований доступ до інформації можливий тільки з використанням штатних апаратних і програмних засобів у наступних випадках: відсутня система розмежування доступу; збій або відмова в інформаційній системі; помилкові дії користувачів або обслуговуючого персоналу інформаційних систем; помилки в системі розмежування доступу; фальсифікація повноважень.

Електромагнітні випромінювання використовуються зловмисниками не тільки для одержання інформації, але й для її знищення. Електромагнітні імпульси здатні знищити інформацію на магнітних носіях. Потужні електромагнітні й надвисокочастотні випромінювання можуть вивести з ладу електронні блоки системи.

Несанкціонована зміна структури системи на етапах розробки й модернізації, так звані «закладки», які в процесі розробки систем впроваджуються, як правило, у спеціалізовані системи, призначені для експлуатації на підприємстві або в державній установі і можуть використовуватися або для безпосереднього шкідницького впливу на інформаційну систему, або для забезпечення неконтрольованого входу в систему.

Одним з основних джерел погроз безпеки інформації в комп'ютерних системах є використання спеціальних програм, що одержали загальну назву шкідливі програми, які залежно від механізму дії поділяють на чотири класи: «логічні бомби»; «черві»; «троянські коні»; «комп'ютерні віруси».

Відносно до інформаційних ресурсів порушники можуть бути внутрішніми (із числа персоналу) або зовнішніми (сторонніми особами).

Внутрішнім порушником може бути особа з наступних категорій персоналу: користувачі (оператори) інформаційної системи; персонал, що обслуговує технічні засоби (інженери, техніки); співробітники відділів розробки й супроводу програмного забезпечення (прикладні й системні програмісти); технічний персонал, що обслуговує будівлі (прибиральники, електрики, сантехники й інші співробітники, що мають доступ у будівлі й приміщення, де розташовані компоненти інформаційної системи); співробітники служби безпеки; керівники різних рівнів посадової ієрархії.

До сторонніх осіб, які можуть бути порушниками відносяться: клієнти (представники організацій, громадяни); відвідувачі (запрошені з будь-якого приводу); представники організацій, взаємодіючих з питань забезпечення життєдіяльності організа-

ції (енерго-, водо-, теплопостачання й т.п.); представники конкуруючих організацій (іноземних спецслужб) або особи, що діють по їх завданню; особи, випадково або, що навмисне порушили пропускний режим (без мети порушити безпеку); будь-які особи за межами контрольованої території.

Можна виділити три основні мотиви їх порушень: безвідповідальність, самоствердження й корисливий інтерес.

При порушеннях, викликаних безвідповідальністю, користувач цілеспрямовано або випадково робить які-небудь руйнуючі дії, не пов'язані зі злим наміром. У більшості випадків це наслідок некомпетентності або недбалості.

Деякі користувачі вважають одержання доступу до системних наборів даних великим успіхом і заради самоствердження у власних очах, або в очах колег затіваючи свого роду гру проти системи.

Порушення безпеки інформаційної системи може бути викликане й корисливим інтересом користувача системи. У цьому випадку він буде цілеспрямовано намагатися подолати систему захисту для доступу до збереженої, переданої і обробленої у системі інформації. Навіть якщо система має засоби, що роблять таке проникнення надзвичайно складним, повністю захистити її від проникнення практично неможливо.

При створенні системи захисту інформації слід враховувати, що вона повинна відповідати наступним найважливішим вимогам:

- запобігання витоку, розкраданню, втратам, викривленню, підробці інформації;
- запобігання несанкціонованих дій щодо знищення, модифікації, викривлення, копіювання, блокування інформації;
- запобігання інших форм незаконного втручання в інформаційні ресурси й інформаційні системи;
- забезпечення правового режиму документованої інформації, як об'єкта власності;
- забезпечення юридичної значимості інформації, наданої у вигляді електронного документа;
- захист конституційних прав громадян на збереження особистої таємниці й конфіденційності персональних даних, наявних в інформаційних системах;
- збереження державної таємниці документованої інформації відповідно до законодавства;
- забезпечення прав суб'єктів в інформаційних процесах і при розробці, виробництві й застосуванні інформаційних систем, технологій і засобів їх забезпечення.

В США був складений, за результатами опитування 214 фірм, перелік застосовуваних заходів для захисту даних, що оброблювалися на засобах електронно-обчислювальної техніки, а також використовуваного програмного забезпечення: парольний захист – 99%, спостереження за роботою – 73%, фізична ізоляція комп'ютерів – 63%, інші – 24%, апаратний захист – 13%, модеми зі зворотним викликом – 6%, різні методи впізнання особистості (сітківка ока, голос і т.д.) – 4%.

Це свідчить, що єдиного надійного методу не існує, як правило, використовується комбінація методів захисту, яка і дає прийнятні результати. Так, відносна непопулярність апаратного захисту говорить про невигідне співвідношення вартості й надійності для апаратних засобів. І, навпаки, такі відносно дешеві й прості засоби, як

парольний захист, фізична ізоляція комп'ютерів, збір статистики роботи, виявляються достатніми з погляду адміністрації [1, с. 137].

Система захисту інформації являє собою комплекс правових, кадрових, організаційно-режимних, апаратних, програмних, криптографічних заходів, що забезпечують її збереження у комп'ютерних системах і комунікаційних мережах від проникнення по каналах технічної розвідки, несанкціонованого доступу, зокрема, з використанням технічних засобів, а також від її втрати внаслідок помилок або некваліфікованих дій користувачів і впливу комп'ютерних вірусів. Кожне підприємство повинне усвідомити необхідність підтримки відповідного режиму безпеки й виділення на ці заходи значних ресурсів.

Для інформаційної безпеки обов'язково повинне бути присутнім правове забезпечення [2, 3]. Воно являє собою сукупність нормативно-правових і підзаконних актів, посадових інструкцій, положень, вимоги яких є обов'язковими в сфері їх діяльності по захисту інформації.

Серед методів захисту інформації особливо виділяються організаційні методи, спрямовані на рішення наступних завдань:

- реалізація на підприємстві ефективного механізму управління, що забезпечує захист конфіденційної інформації й недопущення її витоку;
- здійснення принципу персональної відповідальності керівників підрозділів і персоналу підприємства за захист конфіденційної інформації;
- визначення переліків відомостей, що відносяться на підприємстві до різних категорій конфіденційної інформації;
- обмеження кола осіб, що мають право доступу до різних видів інформації залежно від ступеня її конфіденційності;
- добір і навчання осіб, що призначаються на посади, пов'язані з конфіденційною інформацією;
- організація й ведення конфіденційного діловодства;
- здійснення систематичного контролю над дотриманням установлених вимог по захисту інформації.

Наведений перелік організаційних методів не є вичерпним і, залежить від специфіки діяльності підприємства, ступеня конфіденційності використовуваної інформації, обсягу виконуваних робіт, а також досвіду роботи в області захисту інформації і може бути доповнений іншими методами.

Вважаємо, що однією з найважливіших ланок у забезпеченні системи захисту інформації, є робота з працівниками підприємства, при цьому необхідно:

- забезпечувати довгострокову роботу працівників на підприємстві, виділяти місця й посади відповідно до їх здібностей, боротися з плинністю кадрів;
- створювати матеріальні й моральні стимули, спонукаючи персонал до сумлінної, чесної й творчої роботи, створювати умови для службового зростання й просування на керівні посади найбільш гідних працівників;
- обладнати робочі місця; створювати оптимальний режим праці та відпочинку, дружній інтерфейс (діалог) працівника із системою;
- залучати співробітників до розробки ефективного механізму управління підприємством;
- конструктивно вирішувати конфліктні ситуації, створити гнучку систему звільнення кадрів, яка не травмує людей, спостерігати за новими працівниками.

До організаційно-технічних заходів слід віднести такі:

- здійснювати профілактику комп'ютерних вірусів;
- санкціонувати та контролювати доступ до комп'ютерів (через логін/пароль), кодувати або захищати паролем дані в них;
- використовувати електронні ключі та електронний підпис;
- здійснювати періодично резервне копіювання необхідної інформації, зберігати її в надійному місці;
- обмежити обсяг вихідної інформації до необхідного мінімуму;
- поруч зі справжньою інформацією розміщати неправдиву, розріджувати справжню інформацію, давати її частинами або в загальному вигляді;
- збільшувати обсяг інформації за рахунок надмірних, непотрібних або помилкових даних;
- телефон, електронну пошту використовувати з застосуванням відповідних організаційних і технічних заходів захисту інформації в системах зв'язку, прослуховування;
- обладнати будівлі та приміщення засобами безпеки (пожежної та охоронної сигналізації, телевізійного спостереження та інше);
- використовувати джерела безперебійного енергозабезпечення.

Організаційно-режимні методи вимагають певних дій:

- обмежити місця прийому відвідувачів і постійно їх супроводжувати;
- обмежити кількість стажерів і тимчасових робітників;
- знищувати всі документи, як тільки вони стали непотрібними;
- обмежити доступ до бухгалтерії та носіїв інформації;
- замикати на ключ усі важливі документи наприкінці робочого дня;
- забезпечити охорону приміщень, території та інших об'єктів підприємства;
- організувати надійну, ефективну й жорстку систему контролю за дотриманням норм і правил захисту інформації.

Апаратне забезпечення являє собою технічні засоби захисту інформації – обладнання та прилади, призначені для забезпечення захисту інформації, виключення її витоку, створення перешкод технічним засобам доступу до інформації, що підлягає захисту.

Програмні засоби захисту інформації це різні облікові, статистичні й інформаційні програми, які здатні давати оцінку наявності небезпечних каналів витоку й способів несанкціонованого доступу до конфіденційних даних.

Під криптографічним захистом інформації розуміється таке перетворення вихідної інформації, у результаті якого вона стає недоступною для ознайомлення й використання особами, що не мають на це повноважень. Сучасний криптографічний захист включає розробку систем електронного цифрового підпису, ідентифікації вилучених користувачів, методів захисту від нав'язування неправильних повідомлень і т.д.

Висновки. Захист інформації на сьогодні став по-справжньому гострою й актуальною проблемою, у зв'язку зі швидким і бурхливим розвитком інформаційних технологій. Головна тенденція, яка характеризує його – це збільшення комп'ютерних злочинів і пов'язаних з ними розкрадань конфіденційної інформації, а внаслідок цього й більших матеріальних втрат.

Проблема захисту інформації в сучасному світі визначається наступними факторами: швидке зростання кількості комп'ютерної техніки й розширення її застосування в різних галузях; залучення в процес інформаційної взаємодії все більшого числа

людей і підприємств; відношення до інформації, як до товару, перехід до ринкових відносин, із властивою йому конкуренцією й промисловим шпигунством, в області створення й надання інформаційних послуг; концентрація значних обсягів інформації різного призначення на електронних носіях; кількісне і якісне вдосконалення способів доступу користувачів до інформаційних ресурсів; різноманіття видів погроз і можливих каналів несанкціонованого доступу до інформації; зростання числа кваліфікованих користувачів обчислювальної техніки і можливостей щодо створення ними програмно-математичних впливів на систему.

Інформаційна система, в якій відсутні проблеми в забезпеченні інформаційної безпеки, повинна мати наступні ознаки: мати інформацію різного ступеня конфіденційності; мати криптографічну систему захисту інформації й конфіденційних даних; мати ієрархію повноважень суб'єктів доступу до програм і компонентам інформаційної системи й інформаційних технологій; обов'язкове управління потоками даних у локальних мережах і при їх передачі по каналах зв'язку на значні відстані; наявність системи обліку й реєстрації спроб несанкціонованого доступу, протоколювання подій в інформаційній системі і документів, що виводяться до друку; наявність системи забезпечення цілісності інформації і можливість відновлення інформації; наявність засобів обліку носіїв інформації; наявність фізичної охорони основних засобів і об'єктів інформаційних систем; наявність окремої, спеціальної служби безпеки інформації.

На рівні держави найважливішими завданнями в області забезпечення інформаційної безпеки в Україні, які вимагають термінового вирішення є: подолання технологічного відставання в найважливіших галузях інформатизації, телекомунікацій і зв'язку, що визначають стан національної безпеки; розробка й впровадження технології інформаційної безпеки в системах державного й військового управління, у системах управління екологічно небезпечними виробництвами й критично важливими об'єктами; забезпечення умов для гармонізації національної інформаційної інфраструктури із глобальними інформаційними мережами й системами.

Процес комплексного захисту інформації повинен здійснюватися безупинно на всіх етапах. Реалізація безперервного процесу захисту інформації можлива тільки на основі систем концептуального підходу й промислового виробництва засобів захисту, а створення механізмів захисту і забезпечення їх надійного функціонування й високої ефективності може бути здійснене тільки фахівцями високої кваліфікації в галузі захисту інформації.

Список використаних джерел

1. Экономическая безопасность Российской Федерации: Учебник для вузов.Ч.1./ Под общ. ред. С.В.Степашина. – М.: Издательство «Лань», 2001. – 608 с.
2. Про захист інформації в інформаційно-телекомунікаційних системах,Закон України від 5. 07.1994 року N 81/94-ВР, у редакції від 27.03.2014 року N 1170-VII: zakon.rada. gov.ua› laws/show/80/94-вр
3. Про перелік відомостей, що не становлять комерційної таємниці, постанова КМУ від 09.08.1993р. № 611: http://zakon.rada.gov.ua.

Summary. *The article deals with the problem of information security in the computer systems and networks use; proposed measures to prevent threats to information security and eliminate their consequences.*

Key words: *information security, computer systems, information security threats, security measures: legal, personnel, organizational, hardware, software, cryptographic.*