УДК 338.47

ЛЕГОМІНОВА С. В., к.е.н.,
Державний університет телекомунікацій

ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Розглянуто сучасні проблеми захисту інформації підприємств. Досліджено сутність поняття інформаційна безпека, інформаційна безпека підприємства. Класифіковані основні джерела та суб'єкти загроз, методи і засоби щодо усунення загроз для інформаційних систем. Доведено необхідність створення організаційно-економічного механізму забезпечення інформаційної безпеки підприємства.

Постановка проблеми. Розвиток сфери телекомунікацій є одним із напрямів діяльності сучасного суспільства, що забезпечує надання широкого спектру послуг населенню та характеризується як позитивний чинник розвитку ринку інфокомунікаційних мереж. Світ переживає справжній бум розроблення та впровадження нових методів та технологій передачі, обробки та зберігання інформації, що обумовило глобалізацію телекомунікаційних мереж, створення єдиного світового інформаційного простору. Але стрімке розгортання інфокомунікаційних мереж нового покоління змушує принципово по-новому розглядати роль та значення захисту інформації.

Аналіз останніх досліджень і публікацій. Серед найважливіших досліджень, які висвітлюють різні аспекти генезису інформаційного суспільства та інформаційної безпеки в її загальному значенні слід відзначити значну кількість наукових доробок вітчизняних науковців, серед яких О. Баранов, В. Бегма, К. Бєляков, В. Бакуменко, В. Гавловський, І. Гаврилов, В. Герасименко, О. Гладківський, М. Гуцалюк, В. Домарєв, М. Жулинський, Л. Задорожна, О. Зінченко, В. Малінко, В. Малиновський, Д. Ольшанський, В. Петрик, В. Попов, О. Лактіонова, Г. Лазарєв, А. Марущак, В. Цимбалюк, М. Швец та зарубіжних: Н. Вінер, Б. Ролкер, Л. Дж. Хоффман, К. Шеннон.

Невирішена раніше проблема. Однак, проблема інформаційної безпеки підприємства залишається недостатньо дослідженою. Автори, як правило, пильну увагу приділяють забезпеченню інформаційної безпеці держави, не акцентується увага щодо цілеспрямованого підходу до проблеми захисту інформації в діяльності підприємства. Тому автор в даній роботі намагається проаналізувати питання забезпечення інформаційної безпеки підприємства як суб'єкта інформаційного суспільства. Доцільність подальших досліджень на сьогоднішній момент обумовлена необхідністю розробки стратегії інформаційної безпеки та програми її виконання.

Мета дослідження. Визначити з теоретичної точки зору поняття інформаційної безпеки підприємства відповідно до сучасних тенденцій впровадження новітніх управлінських технологій, обґрунтувати пріоритетні завдання, які спрямовані на збереження та захист інформації у телекомунікаційних мережах загального користування. Розглянути методи та заходи захисту інформації від неправомірних дій. Обґрунтувати засади стосовно організації інформаційної безпеки телекомунікаційних мереж підприємства.

Виклад основного матеріалу. В нашій країні, як і у всьому світі, відбувається поступове становлення інформаційного суспільства, економічною основою якого є створення та вдосконалення технічних і технологічних способів і засобів виробництва, отримання та поширення інформації на основі створення та використання інформаційно-комунікаційних технологій, які можуть розглядатися в якості найважливішої ознаки сучасної інформаційної епохи. Підвищення економічної складової інформаційно-комунікаційних технологій вимагає створення і відповідної правової основи їх виробництва та використання [1, с. 5].

Одним із пріоритетних напрямків державної політики є розвиток інформаційного суспільства в Україні та впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя, що задекларовано Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», Постановою КМУ «Про затвердження Національної системи індикаторів розвитку інформаційного суспільства», Розпорядженням КМУ «Про схвалення Стратегії розвитку інформаційного суспільства» [2, с. 18].

Інформаційні технології визнані рушієм далекосяжних структурних змін, що забезпечує швидкий прогрес країни, її політики та економіки, розвиток суспільства і добробут його грома-

дян. Розвиток і застосування інформаційних технологій значно спрощує вирішення проблеми безробіття та зайнятості населення, збільшує можливості для самоосвіти, набуття додаткових спеціальностей, обміну корисними відомостями щодо діяльності у будь-якій сфері народного господарства [3]. Сучасні інформаційні системи та технології є засобом підвищення продуктивності та ефективності роботи працівників.

Все більшого значення набуває забезпечення інформаційної безпеки підприємства. Це пов'язано із зростаючим обсягом інформації, вдосконаленням засобів її зберігання, передачі та обробки. Наявність значної частини інформації в електронній формі, використання локальних і глобальних мереж створюють якісно нові загрози конфіденційної інформації.

Наукова література не визначає єдиного погляду на зміст поняття «інформаційна безпека» та «інформаційна безпека підприємства».

Інформаційна безпека — захищеність (стан захищеності) основних інтересів особистості, суспільства і держави в сфері інформації, включаючи інформаційну і телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі, як повнота, об'єктивність, доступність і конфіденційність.

Слід відзначити, що задоволення в будь-якій мірі потреб в інформації призводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок — обґрунтованість рішень та дій, що приймаються.

В. Цимбалюк характеризує інформаційну безпеку як стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації [4, с. 3].

В. Фурашев вважає, що інформаційна безпека — це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності [5, с. 48].

С. Гуцу визначає інформаційну безпеку як стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [6, с. 35].

О. Литвиненко, під інформаційної безпекою розуміє єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності [7, с. 9].

Сороківська О. А. визначає інформаційну безпеку підприємства як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [8].

М. Танцюра характеризує інформаційну безпеку підприємства як збереження конфіденційності, цілісності та доступності інформації. Доступність — це властивість бути досяжним та придатним до використання авторизованими сутностями; цілісність — це властивість захищеності точності та повноти даних; конфіденційність — це властивість захищеності інформації від неавторизованого використання фізичними особами, сутностями та процесами. Інформаційні активи — це знання чи дані, які мають цінність для організації [9, с. 452].

Враховуючи дані визначення, слід погодитись з визначенням А. Марущак, що інформаційна безпека підприємства — це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток [10, с. 94].

Отже, підсумовуючи вище зазначене, вважаємо за необхідне наголосити, що пріоритетним напрямом у процесі забезпечення інформаційної безпеки підприємства є збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг.

Аніловська Г. Я. одним із методів забезпечення інформаційної безпеки підприємства називає стандартизацію інформаційної структури інформаційної системи, елементами якої є форми існування і подання інформації у цілому, а зв'язками — операції перетворення інформації в системі. Стандартизація цього типу полягає у запровадженні єдиних правил введення, зберігання, аналізу, оброблення інформації [11].

Таким чином, під інформаційною безпекою розуміється захищеність інформації та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може бути нанесення збитку самій інформації, її власникам або підтримуючій інфраструктурі.

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 [12].

Також необхідно враховувати, що загроза інформаційним системам підприємства може настати з боку наступних суб'єктів:

• працівники підприємства, що використовують своє службове становище (коли законні права за посадою використовуються для незаконних операцій з інформацією);

• працівники підприємства, що не мають права в силу своїх службових обов'язків, але здійснили несанкціонований доступ до конфіденційної інформації;

• особи, які не пов'язані з підприємством трудовою угодою (контрактом).

Всі методи забезпечення інформаційної безпеки підприємства можна об'єднати у три групи: правові, організаційні та програмно-технічні [17].

Правові методи включають сукупність нормативно-правових актів, які регулюють відносини, пов'язані з використанням інформації в діяльності підприємства. З розвитком правового регулювання процесів інформаційного обміну набагато простіше встановлювати партнерські стосунки, шукати контрагентів, реалізовувати і закуповувати продукцію, стали доступніші нові «види бізнесу» — нові форми здійснення підприємницької діяльності. Захист інформації є невід'ємної складової бізнесу.

Програмно-технічні методи реалізуються за допомогою засобів програмного та апаратного забезпечення. Технічні методи захисту припускають використання засобів програмно-технічного характеру, спрямованих, передусім, на обмеження доступу користувача, який працює з інформаційними системами підприємства, до тієї інформації, звертатися до якої він не має права [18, с. 46-47].

Організаційні методи полягають в забезпеченні збереження конфіденційної інформації підприємства шляхом формування корпоративної системи захисту і пов'язані з обмеженням можливого несанкціонованого фізичного доступу до інформаційних систем.

Незважаючи на використання вищезазначених методів, забезпечення інформаційної безпеки підприємства на належному рівні можливе лише тоді, коли інформаційна складова економічної безпеки розглядатиметься як невід'ємний елемент процесу управління підприємством.

Захист інформації, забезпечення інформаційної безпеки повинно носити системний характер, тобто різні засоби захисту (апаратні, програмні, фізичні, організаційні) повинні застосовуватися одночасно і під єдиним управлінням. Існує велика кількість інструментів забезпечення інформаційної безпеки: засоби ідентифікації та автентифікації користувачів; засоби шифрування інформації, міжмережні екрани; віртуальні приватні мережі; засоби контентної фільтрації; інструменти перевірки цілісності вмісту дисків; засоби антивірусного захисту; системи виявлення вразливостей мереж і аналізатори мережних атак. Особливе місце займають криптографічні методи для захисту інформації. Інтерес комерційних структур до них значно зріс у зв'язку зі зменшенням вартості перехоплення інформації, що передається електронною поштою чи функціонує в системі електронних платежів. Найпоширенішими вважаються методи кодування та шифрування інформації. Поряд з ними використовуються методи розділення та стиснення даних. У процесі захисту передачі усної інформації використовують методи аналогового скемблірування та дискретизації мови з подальшим шифруванням.

Один із перспективних напрямів захисту інформації сформулювали сучасні методи стенографії, що базуються на різних принципах, забезпечують таємницю самого факту існування секретної інформації в тому чи іншому середовищі за допомогою відповідних засобів: невидимих чорнил, мікрофотознімків, таємних каналів та засобів зв'язку з плаваючими частотами тощо. Незважаючи на використання зазначених методів, забезпечення інформаційної безпеки підприємства на належному рівні можливе лише тоді, коли інформаційна складова економічної безпеки розглядатиметься як невід'ємний елемент процесу управління підприємством.

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. Більш того, володіючи складними апаратними засобами захисту інформації, більшість підприємств навіть напо-

ловину не використовують їх потенціал. Переважна більшість вимог стандартів інформаційної безпеки можуть бути реалізовані наявними у фірм засобами захисту [12].

Таким чином, 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 [13].

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 [13].

Важливим є визначення етапів побудови політики інформаційної безпеки, а саме:

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 [14].

На практиці інформаційна безпека включає сукупність напрямів, методів, засобів і заходів, що знижують вразливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку.

Структура системи залежить від об'єму та цінності інформації, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи. Більшість фахівців у галузі захисту інформації вважають, що інформаційна безпека підтримується на належному рівні, якщо всі інформаційні ресурси системи дотримуються відповідного рівня конфіденційності, цілісності (неможливості навмисної або випадкової її модифікації) і доступності.

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 [15].

Фахівці-практики виділяють, наприклад, такі основні напрями технічного захисту інформаційних систем [16, с. 54]:

- захист інформаційних ресурсів від несанкціонованого доступу і використання — використовуються засоби контролю включення живлення і завантаження програмного забезпечення, а також методи парольного захисту при вході в систему;

- захист від витоку по вторинних каналах електромагнітних випромінювань і наведень — за допомогою екранування апаратури, приміщень, застосуванням маскуючих генераторів шумів, додатковою перевіркою апаратури на наявність компрометуючих випромінювань;

- захист інформації в каналах зв'язку і вузлах комутації — використовуються процедури аутентифікації абонентів і повідомлень, шифрування і спеціальні протоколи зв'язку;

- захист юридичної значущості електронних документів — при довірчих стосунках двох суб'єктів підприємницької діяльності і коли виникає необхідність передачі документів (платіжних доручень, контрактів) по комп'ютерних мережах — для визначення істинності адреса-

та документ доповнюється «цифровим підписом» — спеціальною міткою, нерозривно логічно пов'язаною з текстом і формованою за допомогою секретного криптографічного ключа; захист автоматизованих систем від комп'ютерних вірусів і незаконної модифікації — застосовуються імуностійкі програми і механізми модифікації фактів програмного забезпечення.

Висновки та перспективи подальших досліджень. Отже, використання інформаційних технологій значно підвищує ефективність процесів, зменшує затрати на їх проведення, проте зумовлює виникнення нових загроз для функціонування підприємства. Реалізовуючи системний підхід до інформаційної безпеки підприємства слід дотримуватись принципів конфіденційності, цілісності та доступності інформації, що дозволить підвищити результативність. Забезпечення інформаційної безпеки слід розглядати як невід'ємний елемент процесу управління підприємством.

Список використаних джерел

*1. **Журавлев, Ю. А.** Правовые основы обеспечения информационной безопасности юридических лиц: автореф. дисс. на соискание ученой степени канд. юрид. наук: спец. 12.00.14. «Административное право, финансовое право, информационное право» / Ю. А. Журавлев.— Москва, 2009.— 26 с.*

*2. **Доповідь** Кабінету міністрів України Верховній Раді України «Про стан та перспективи розвитку інформатизації в Україні за 2012 рік», Київ.— 2012.*

*3. **Брайсон, Джон М.** Стратегічне планування для державних та неприбуткових організацій: пер. з англ. А. Кам'янець / Джон М. Брайсон.— Львів: Вид-во «Літопис», 2004.— 352 с.*

*4. **Цимбалюк, В. С.** Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті / В. С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.— 2004.— №8.— С. 30–33.*

*5. **Фурашев, В. М.** Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки / В. М. Фурашев // Інформація і право: науковий журнал.— К.: НДЦПІ НАПрН України, 2012.— № 1(4).— С. 46–56.*

*6. **Гуцу, С. Ф.** Правові основи інформаційної діяльності: навчальний посібник / С. Ф. Гуцу.— Х.: Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009.— 48 с.*

*7. **Литвиненко, О. В.** Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії): автореф. дис. на здобуття наук. ступеня канд. політ. наук: спец. 23.00.04. / О. В. Литвиненко.— К., 1997.— 18 с.*

*8. **Сороківська, О. А.** Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко.— [Електронний ресурс].— Режим доступу: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf*

*9. **Тацюра, М. Ю.** Проблемні аспекти стандартизації у галузі інформаційної безпеки підприємства // Матеріали Другої наук.-практ. конф. «Сталий розвиток та екологічна безпека суспільства в економічних трансформаціях» 23–24 вересня 2010 р. м. Бахчисарай, НДІ сталого розвитку та природокористування, РВПС України НАН України, Кримський інститут КНЕУ ім. Вадима Гетьмана / М. Ю. Тацюра.— Сімферополь: Фенікс, 2010.— С. 451–453.*

*10. **Марущак, А. І.** Інформаційно-правові напрями дослідження проблем інформаційної безпеки // Державна безпека України / А. І. Марущак.— 2011.— № 21.— С. 92–95.*

*11. **Аніловська, Г. Я.** Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. [Електронний ресурс].— Режим доступу: http://www.nbuv.gov.ua/portal/chem_biol/nvnltu/18_9/270_Anilowska_18_9.pdf*

*12. **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*

*13. **Власова, Л. А.** Защита информации/ Л. А. Власова.— Хабаровск: РИЦ ХГАЭП, 2007.—84 с.*

*14. **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.*

*15. **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/*

*16. **Степанов, Е. М.** «Кроты» на фирме (персонал и конфиденциальная информация) // Предпринимательское право / Е. М. Степанов.— 1999.— № 4.— С. 53–56.*

17. ***Гриджук, Г. С.*** *Систематизація методів інформаційної безпеки підприємства.— [Електронний ресурс].— Режим доступу:*

http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/64.pdf

18. ***Казакевич, О. Ю.*** *Предприниматель в опасности: способы защиты. Практическое руководство для предпринимателей и бизнесменов / О. Ю. Казакевич, Н. В. Конев.— М.: Юрфак МГУ, 2011.— 152 с.*

Легоминова Светлана Владимировна*. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ. Рассмотрены современные проблемы защиты информации предприятий. Исследовано сущность понятия информационная безопасность, информационная безопасность предприятия. Классифицированы основные источники и субъекты угроз, методы и способы их устранения. Доказано необходимость создания организационно-экономического механизма обеспечения информационной безопасности предприятия.*

Legominova Svetlana*. THE THEORETICAL BASIS OF INFORMATION SECURITY ENTERPRISE. The modern problems of information security companies. The essence of the concept of information security, information security company. Classified main sources and subjects of threats, methods and means to address threats to information systems. The necessity of creating organizational and economic mechanism to ensure information security.*