УДК 339.9

Качан О.І., асист.
Науковий керівник – д.е.н., проф. **О.М. Сазонець**
Національний університет водного господарства та природокористування, м. Рівне

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА В УМОВАХ ГЛОБАЛІЗАЦІЇ

Поняття загрози інформаційної безпеки зародилось майже у той же час, як і поява інформаційного середовища. Спочатку це були прояви крадіжки інформації з комп'ютера, незаконне використання, порча інформації на комп'ютерах. Пізніше з розвитком інформаційних мереж інформаційна небезпека перетворилась в засоби перекачування по мережі неправдивої інформації, вірусів. Зараз питання безпеки відноситься майже до всіх агентів глобального інформаційного середовища. Україна як активний учасник процесів циклу життя інформації не стоїть в стороні від них. Це відбувається як на загальному міжкраїновому рівні, так і в середині кожного окремого підприємства.

Існує декілька визначень поняття «інформаційна безпека підприємства». Зокрема, Цимбалюк В. дає таке визначення - це суспільні відносини щодо створення та підтримання на належному (бажаному, можливому) рівні життєдіяльності відповідної інформаційної системи, у тому числі підприємництва [1].

Сороківська О. А. розглядає поняття «інформаційна безпека підприємства» як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [2].

Танцюра М.Ю. дане поняття трактує як відношення рівня інформаційного захисту до рівня інформаційних загроз; сукупність засобів та дій уповноважених осіб спрямованих на захист інформаційних ресурсів та інформаційної інфраструктури даного підприємства в процесі обміну, обробки та зберігання інформації на всіх рівнях інформаційної системи підприємства [3, с.5].

Крюков О.І. визначає «інформаційна безпека» – це суспільні правовідносини щодо процесу організації створення, підтримки, охорони та захисту необхідних для особи (людини чи юридичної особи, установи, підприємства, організації), суспільства і держави безпечних умов їх життєдіяльності; суспільні правовідносини пов'язані з організацією технологій створення, розповсюдження, зберігання та використанням інформації (відомостей, даних, знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, суспільства, держави [4,с.3].

На сьогоднішній день нагальною постає проблема збільшення інформаційної безпеки підприємства, яка значною мірою залежить від ступеня захищеності інформаційної сфери. Рівень інформаційної безпеки впливає на розвиток та впровадження науково-технічних інновацій у процеси виробництва, збереження стабільності функціонування можливості економічного зростання.

Розвиток бізнесу перебуває у постійному русі і динамічно змінюється під впливом конкуренції та процесів глобалізації. Глобальний етап інтеграції економічних систем безпосередньо пов'язаний з багатоплановим процесом розширення та поглиблення світогосподарських зв'язків завдяки підвищенню мобільності факторів і результатів виробництва (макрорівень) та залучення фірми до міжнародних операцій (мікрорівень) [5,с.9]. Під впливом глобальних процесів

спостерігається прискорення науково-технічного прогресу, розширюється обмін новими, зокрема, збільшується кількість здійснення фінансових видів послуг. Проте під швидкими темпами зростання економічних процесів при здійсненні господарської діяльності зростає і роль інформаційної безпеки підприємства.

При веденні своєї діяльності підприємець обов'язково наштовхується на необхідність отримання, обробки, зберігання, перетворення, передачі та ліквідації непотрібної інформації. Якщо деяка інформація є цінною для підприємця, то її треба охороняти від зловмисників. Цінність визначається через ряд параметрів, до яких належать корисність, достовірність, своєчасність, релевантність. При захисті інформації слід перекрити всі канали можливого витоку та забезпечити безпеку зберігання інформації на усіх носіях, що маються на підприємстві. Загрози інформаційної безпеки поділяються на внутрішні та зовнішні.

Зовнішні зловмисні дії можуть бути такими:

– копіюванні цінних документів, або викрадення файлів;
– викрадення флеш-карт;
– викрадення інформації у процесі її передавання по мережі Інтернет;
– пошкодження носіїв з інформацією;
– донесення інформації до фірм-конкурентів, або взагалі до іншої країни;
– викрадення інформації за допомогою інсайдерів;
– переманювання персоналу на іншу фірму.

До найбільш поширених внутрішніх загроз відносяться крадіжка, зараження інформації вірусами, або порча файлів службовцями компанії. До причин внутрішніх загроз відносяться:

– причини психологічного характеру у зв'язку з відносинами між співробітниками підприємства, що не склалися;
– незадоволення рівнем заробітної плати;
– недобрі відносини між співробітником та керівництвом компанії;

Психологи стверджують, що біля 25 % всіх співробітників підприємств розголошують інформацію, продають або передають її конкуруючим компаніям задля додаткового заробітку.

Захист інформації на підприємстві є дуже важливою річчю і цей аспект повинен бути обов'язковим при укладанні контракту компанією з її працівником, особливо якщо цей працівник займає керуючу посаду в компанії.

Небезпека, в першу чергу, загрожує інформації, яка зберігається в інформаційних системах підприємства. У цю систему входять програмне забезпечення автоматизованої системи, програми для виконання конкретних задач компанії, програмні оболонки, текстові редактори, пакети програм, бази даних. Інформація може поступати по локальній мережі з пристрою введення, а саме з клавіатури, з зовнішнього середовища, а саме з мережі Інтернет, по системі SWIFT, від інших компаній.

Щоб гарантувати безпеку інформаційної системи підприємства, необхідним є наділення повноважень зареєстрованим користувачам, серед яких можуть бути як певні особи, так і організації. Ці користувачі можуть здійснювати тільки визначені наперед дії з використанням інформаційних технологій.

Небезпека інформації на підприємстві виникає з певних джерел (рис 1.).

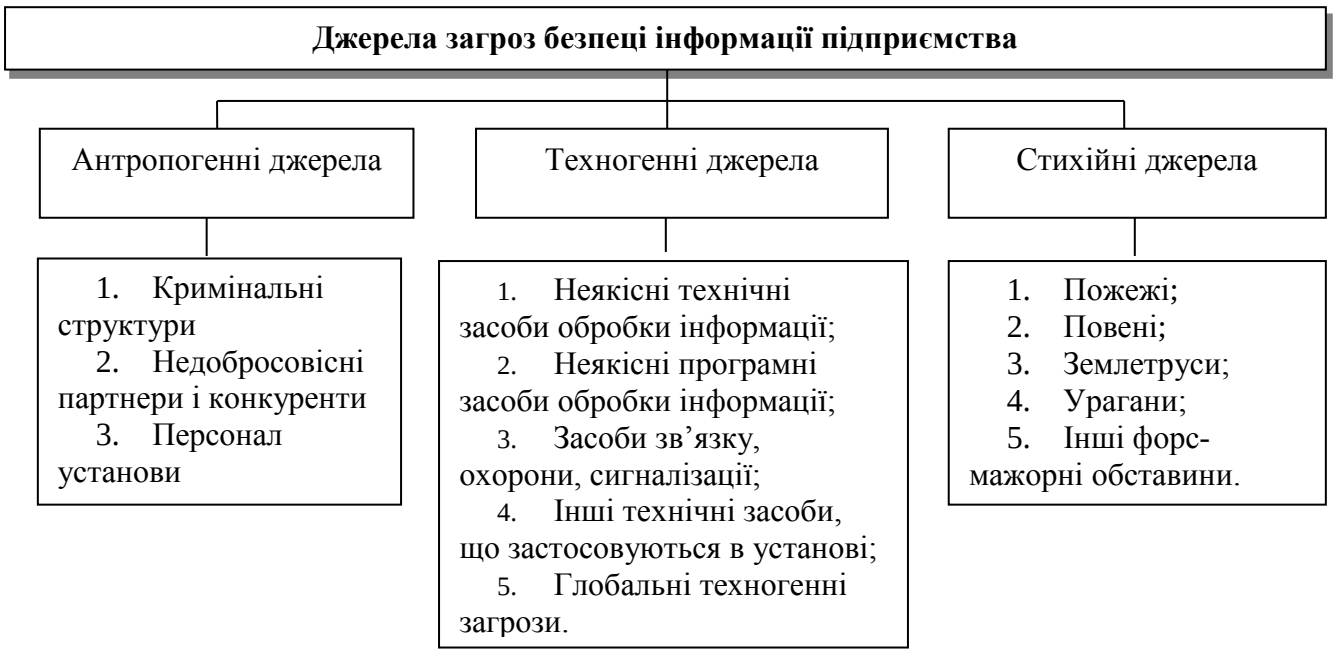

Рис. 1 *Джерела загроз безпеці інформації підприємства*

Аналізуючи завдання захисту інформації, введемо поняття обчислювального середовища, в якому відбувається обробка даних за допомогою обчислювальних програм. Дані і обчислювальні програми при цьому знаходяться на внутрішніх носіях. Під операційним середовищем розуміємо сукупність елементів обчислювального середовища, які знаходяться в оперативній пам' яті комп' ютера. Захист елементів обчислювального середовища практично зводиться до захисту даних та програм. Засоби захисту інформації інформаційної системи містять захист елементів обчислювального середовища та контроль елементів операційного середовища

Захист елементів обчислювального середовища включає:

- захист даних;
- засоби власного захисту програм;
- захист процедур обробки інформації.

Контроль елементів оперативного середовища містить:

- контроль зовнішніх компонент операційного середовища;
- контроль цілісності внутрішніх компонент операційного середовища;
- контроль семантики даних.

Захист інформації здійснюється різними способами. До низ відносяться захист програм від читання та копіювання, захист авторських прав на інформацію, захист від несанкціонованого доступу і запуску програм, самотестування і самовідновлення коду програм, що виконується.

Питання авторських прав є питанням захисту інтелектуальної власності, якому приділяють першочергову увагу розробники програм. Захист програм від копіювання призначається за допомогою програмних засобів, при цьому використовується ідентифікація користувача, обмеження на кількість запусків програми, обмеження датою запуску, або кількістю запусків. Самотестування і самовідновлення коду програм здійснюється за допомогою введення модулів діагностики характеристик коду програми. Ними є розмір файлу, перелік контрольних точок, контрольна сума

тощо. Також використовуються алгоритми, що відновлюють штатний код програми при необхідності.

Отже, в умовах глобалізації забезпечення інформаційної безпеки на підприємстві полягає постійному контролі за джерелами виникнення потенційних загроз (антропогенні, технологічні та стихійні джерела) та необхідності здійснювати захист інформації різними способами (захист програм від читання та копіювання, захист авторських прав на інформацію, захист від несанкціонованого доступу і запуску програм, само тестування).

Список використаних джерел:

1. *Цимбалюк В. Інформаційна безпека підприємницької діяльності, визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації) //Підприємництво, господарство і право. – 2004.-№3./С.88-91*
2. *Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи [Текст] / О. А. Сороківська, В. Л. Гевко // Вісн. Хмельниц. нац. ун-ту. Сер.: Екон. науки. – 2010. – № 2. – Т. 2. – С. 32–35.*
3. *Танцюра М.Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства (на прикладі туристичних підприємств АР Крим): автореф. дис.на здобуття наук ступеня канд. екон. наук: 08.00.04//М.Ю. Танцюра.- Сімферополь, 2012.-21*
4. *Крюков О.І. Інформаційна безпека держави в умовах глобалізації / О. І. Крюков. // Державне будівництво. - 2007. - № 2. Режим доступу: http://nbuv.gov.ua/UJRN/DeBu_2007_2_12*
5. *Лук'яненко Д. Г. Стратегії глобального управління / Д. Г. Лук'яненко, Т. В. Кальченко // Міжнародна економічна політика. – 2009. – № 8-9. – С. 5-43.*