УДК 004.056

Гой В. О., здобувач вищої освіти;
Анісімова О. М., д-р екон. наук, професор,
завідувач кафедри інформаційних технологій,
Донецький національний університет імені Василя Стуса

ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Ключові слова: інформація, захист інформації, підприємство, організації, дані, закони, конфіденційність.

Вступ. Сучасний інформаційний світ «наполягає» на важливості захисту інформації, що є одним із найважливіших етапів створення документації. Частково це пов'язано зі швидким розвитком інформатизації підприємств та особливою активністю порушників.

Актуальність. Тема захисту інформації на підприємстві є надважливою й актуальною. Компанії збільшуються, відбувається постійний потік людей, звільнення, стажування, не завжди люди є чесними й відкритими, а інколи і створюють спеціальні умови для використання інформації підприємства з власною метою. Тому керівництво повинно повністю забезпечити захист даних на усіх рівнях: і документів на матеріальних носіях, і інформації на електронних.

За законодавством, а саме у ст. 1 ЗУ «Про інформацію», зазначено таке визначення: «Інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [1].

Саме ж поняття інформація – ознайомлення, пояснення, є багатоаспектним у всіх сферах життєдіяльності. Кожен у нашій країні має право на інформацію, що дає можливість вільно одержувати її, використовувати, а також поширювати й зберігати інформацію. Важливим є захист інформації, який необхідний для реалізації прав людини, свободи й законних інтересів.

Інформація існує у різних формах і має різні види носіїв: книги, ілюстрації, звукові записи, бази даних. Усі форми повинні мати гарантію їх захисту. У вирішенні цього питання важливу роль відіграє конфіденційність, цілісність, доступність, і ці властивості мають враховуватись під час правового захисту.

Щодо поняття захист інформації, яке також затверджене у ст. 1 ЗУ «Про інформацію», захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [1].

Захист інформації розуміють як захист від ознайомлення, модифікації, копіювання, знищення та інше.

Захист інформації повинен забезпечувати конфіденційність, цілісність і доступність інформації, а також технічний захист в інформаційному просторі.

Головною метою підприємства є забезпечення безпеки саме таких аспектів:

- усіх наявних баз даних, що містять важливі відомості;
- документообігу підприємства, що здійснюється в електронному вигляді;

• різних технічних аспектів, які пов’язані із інформаційною інфраструктурою підприємства;

• комерційних питань, зокрема конфіденційних даних про бізнес-процеси [2].

Отримання таких відомостей сторонньою організацією, підприємством, державою чи конкретною людною може призвести до серйозних наслідків, навіть до руйнування. Тому дуже важливо мати висококваліфікованих спеціалістів, відповідальних за комплексний захист інформації на підприємстві та її належний контроль.

Постає питання, які ж є джерела спотворення й загроза інформації. Загрозою є будь-які обставини та події, які можуть причинити порушення політики безпеки інформації й нанесення збитку автоматизованій системі [3].

Загрози поділяють на: наслідки стихійних лих і техногенних катастроф, відмови обладнання, наслідки помилок персоналу, наслідки помилок системи захисту, навмисні дії порушників. Детально класифікація загроз знищення інформації наведена на рисунку 1:

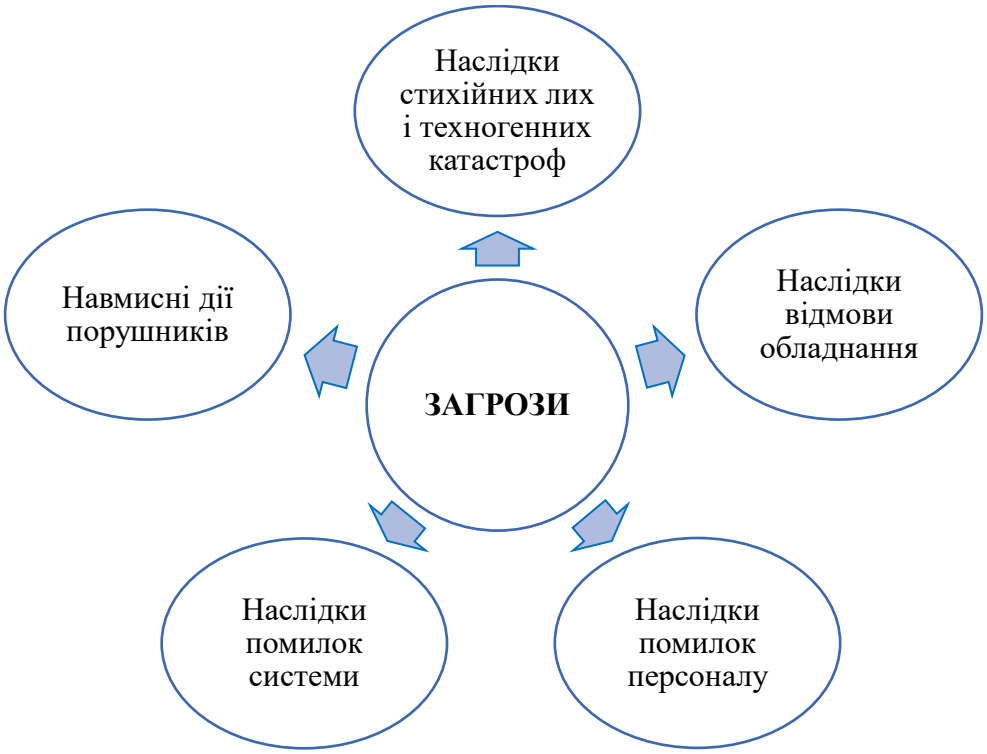

Рисунок 1 – Класифікація загроз знищення інформації

- Наслідки стихійних лих і техногенних катастроф (методи боротьби – резервування апаратного забезпечення, резервні копії).

- Наслідки відмови обладнання (методи боротьби – резервування, копії, вибір надійного постачальника апаратного забезпечення).

- Наслідки помилок персоналу (методи боротьби – ретельне добирання персоналу, навчання, створення систем адміністративних стягнень за порушення, створення позитивної атмосфери всередині колективу).

- Наслідки помилок системи захисту (методи боротьби – залучення ліцензованих спеціалістів, експертиза проєкту, періодичний аудит системи захисту).
- Навмисні дії порушників (методи боротьби зазвичай залежать від способу дій) [4].

У теорії доведено, якщо система захисту інформації побудована за попередньо описаною схемою, і частіше навмисні дії порушників у такій системі неможливі. Але все ж жодна з систем захисту не дає гарантії й не може довгий час протидіяти цілеспрямованим діям сучасних технологій, а особливо, коли діє кваліфікований порушник [5].

Висновки

Отже, інформація обов'язково повинна бути захищеною, захист інформації є дуже кропітким та відповідальним процесом. Захист інформації є найактуальнішим питанням сьогодення й важливим завданням через технологічні можливості сучасного світу. Проблема набуває гостроти щоденно, тому до неї потрібно підходити комплексно, робити аналіз, досліджувати проблематику, а також користуватись усіма можливостями реального світу, наймати ІТ-професіоналів, юридичних консультантів і інших спеціалістів, які можуть забезпечити підприємству, організації повний захист інформації.

Важливо дотримуватись усіх методів захисту інформації, слідкувати і контролювати систему захисту на постійній основі, адже інформаційні технології розвиваються дуже швидко і стрімко розповсюджуються.

Список використаних джерел

1. Закон України від 1992.10.02 № 2657-XII «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

2. Головльов С. Захист інформації на підприємстві – забезпечення безпеки даних та подолання ризиків. URL: https://resit.com.ua/zachist-informacii-na-pidpriemstvi/

3. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека: Термінологічний навчальний довідник / за ред. В. Г. Кривуци. Київ. 2004. 508 с.

4. Логінова Н. І., Дробожур Р. Р. Правовий захист інформації: навчальний посібник. Одеса. 2015. 264 с.

5. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації: навчальний посібник. Харків: Вид. ХНЕУ, 2013. 476 с.