# Результати аналізу загроз інформаційній безпеці компаній

**О. В. Шацька,** ДІД-21
**С. В. Гаркуша,** д. т. н., доцент  науковий керівник

Інформаційна безпека на сьогоднішній день є важливою темою дослідження, так як загальна комп'ютеризація основних сфер діяльності призвела до появи широкого спектру внутрішніх і зовнішніх загроз, нетрадиційних каналів втрат інформації і несанкціонованого доступу до неї.

Під інформаційною безпекою розуміють комплекс організаційних, технічних і технологічних заходів щодо захисту інформації від несанкціонованого доступу, її руйнування, модифікації, розкриття і затримок у доступі [1].

В ході досліджень були сформульовані головні цілі інформаційної безпеки, до яких слід віднести:

- захист національних інтересів;
- забезпечення людини і суспільства достовірною та повною інформацією;
- правовий захист людини і суспільства при отриманні, поширенні та використанні інформації.

Крім того можна виділити три основні складові інформаційної безпеки:

- доступність – забезпечення своєчасного і надійного доступу до інформації та інформаційних сервісів;
- цілісність – відсутність неправомірних спотворень, доповнення або знищення інформації;
- конфіденційність – стан доступності інформації тільки авторизованим користувачам, процесам і пристроям.

Основним об'єктом інформаційної безпеки виступають інформаційні ресурси. Кожна компанія має інформаційні ресурси (блок 1) – знання та вміння співробітників, апаратне і програмне забезпечення, документацію та інші види інформації. Важливою складовою ресурсу компанії є інформація про неї в суспільстві, яка формує її репутацію, ступінь довіри з боку клієнтів, престиж тощо.

Втрата інформаційних ресурсів відбувається при порушенні конфіденційності, працездатності, цілісності та повноти (блок 3). Чим цінніша інформація в компанії, тим більша небезпека з боку зовнішніх та внутрішніх шкідливих дій, спрямованих на заволодіння нею або на її знищення. У табл. 1 наведені основні шкідливі дії, що можуть вчинятися правопорушниками, а також засоби боротьби з ними [2].

**Таблиця 1 – Основні шкідливі дії та засоби боротьби з ними**

| **Вид правопорушення** | **Засоби боротьби** |
|---|---|
| Підміна особистості | Аутентифікація |
| Фальсифікація даних | Авторизація |
| Відмова від авторства | Заборона на анонімні операції, аудит, цифровий підпис |
| Розкриття інформації | Уникати передачі секрету по мережі, використовувати захищені (шифровані) протоколи |
| Підвищення привілеїв | Використовувати привілеї мінімально достатні для виконання завдання |

Наявність описаних засобів визначає ступінь загроз безпеці, тобто вони виступають похідним показником вразливості. Зазначені засоби збільшують потенційні дії та ведуть до вимог, що відповідають заходам безпеки, які повинні гарантувати конфіденційність, цілісність, доступність інформації, своєчасну звітність, фізичну безпеку і контроль доступу (блок 5). У свою чергу, заходи безпеки можуть бути технічними, організаційними та управлінськими (блок 6).

Наприклад, захист від вірусів може бути реалізований технічно за допомогою установки антивіруса, а може бути вирішений організаційно шляхом заборони доступу до мережі Інтернет, самовільної установки програмного забезпечення і використання мобільних накопичувачів інформації.

Заходи безпеки забезпечуються різними системами: процедурної, фізичної, системної, комунікаційної безпеки та безпеки персоналу (блок 7). Таким чином, вони зменшують ризики шляхом захисту від загроз.
Крім того, на рис. 1 наведені джерела загроз: навмисні дії з боку людей, можливі аварії (помилки в роботі користувачів, програм та обладнання), а також природні фактори (блок 8).

Необхідно зазначити, що в категорію вандалів і терористів (які становлять небезпеку з точки зору крадіжки та пошкодження інформації) потрапляють також журналісти (блок 9). Втім, очевидно, що в плані витоку корпоративної інформації журналісти часом представляють не меншу небезпеку для компанії, ніж шпигуни. Одним із засобів боротьби з цим явищем є надання прав спілкування з журналістами лише певним категоріям співробітників – зазвичай вищому менеджменту і співробітникам відділу маркетингу [3].

В ході дослідження встановлено, що забезпечення інформаційної безпеки є комплексним завданням. Це обумовлюється складністю інформаційного середовища як багатопланового механізму, в якому діють компоненти, як електронного обладнання та програмного забезпечення, так і персоналу. Вирішення проблеми забезпечення інформаційної безпеки реалізовується шляхом застосування законодавчих, організаційних і програм-но-технічних заходів. Нехтування хоча б одним з аспектів цієї проблеми може призвести до втрати або витоку інформації, вартість і роль якої в житті сучасного суспільства набуває все більш важливого значення.

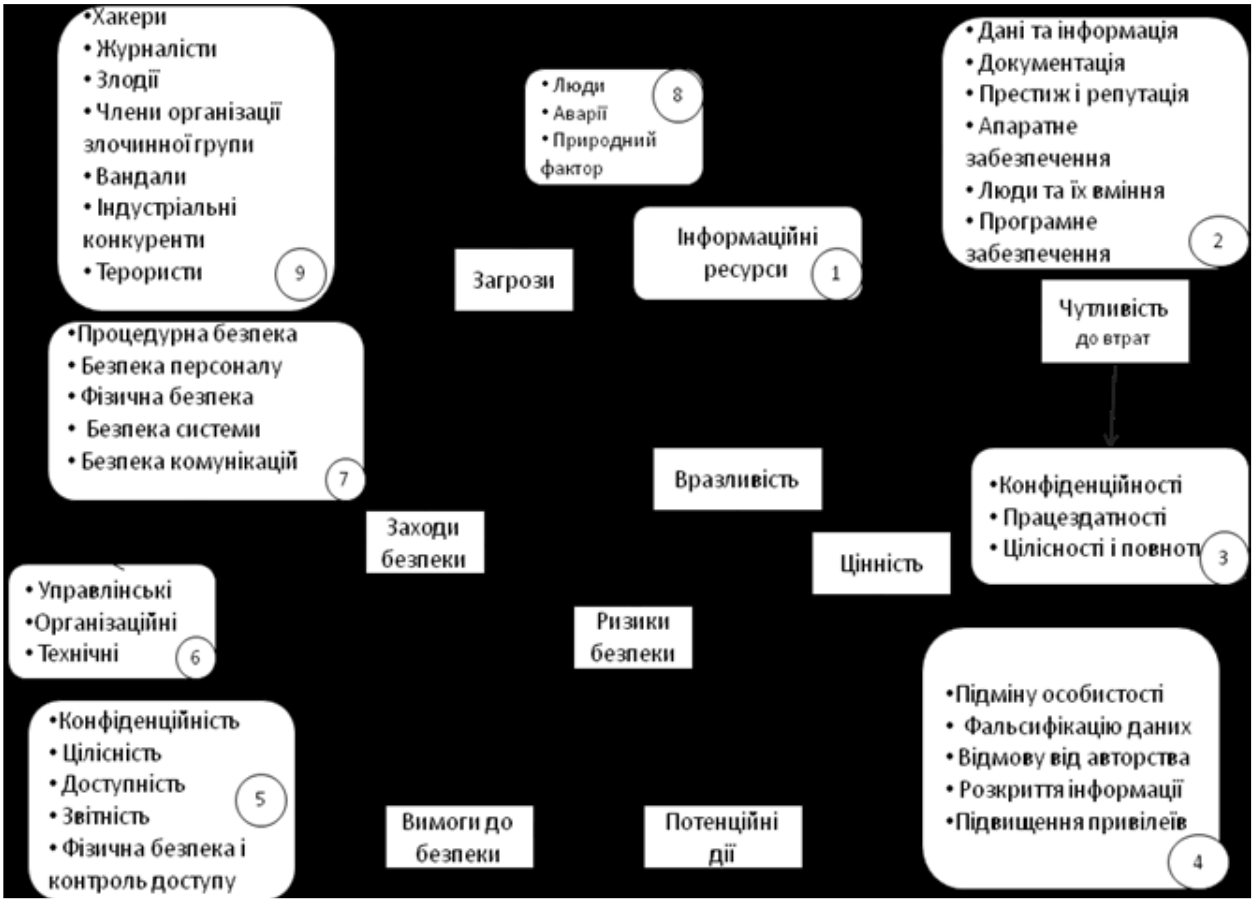


Рисунок 1 – Схема впливу різноманітних факторів на безпеку інформаційних ресурсів

**Список використаних джерел**

1. Аскеров Т. М. Защита информации и информационная безопас-ность : учеб. пособие / Т. М. Аскеров, К. И. Курбако.  Москва : Российская экон. акад., 2013  387 с.

2. Бармен С. Д. Розробка правил інформаційної безпеки / С. Д. Бар-мен. – Москва : Вільямс, 2013. – 208 с.

3. Малюк А. А. Теорія захисту інформації : навч. посіб. / А. А. Ма-люк. – Київ : МАУП, 2014. – 368 с.