УДК 330.131.7

В.В. Іванієнко[1]

*5531viktor@ukr.net*

[1]*Харківський національний університет ім.. С.Кузнеця, Харків*

# ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ УМОВАХ ГОСПОДАРЮВАННЯ

У будь-якій галузі базовий принцип інформаційної безпеки полягає в дотриманні балансу інтересів суб'єкта господарювання, громадянина, суспільства і держави. З урахуванням цього будується система інформаційної безпеки підприємства, яка повинна враховувати можливі загрози і методи захисту інформації. До загроз відносять:

1. Неуважність і недбалість співробітників. Завжди є ймовірність того, що хто-небудь відкриє фішингових лист і впровадить вірус з особистого ноутбука на сервер компанії. Або скопіює файл з конфіденційною інформацією на планшет, флешку або КПК для роботи у відрядженні. І жодна компанія не застрахована від пересилання неуважним співробітником важливих файлів не за тією адресою.

2. Використання піратського ПЗ. Неліцензійні програми не дають захисту від шахраїв, зацікавлених в крадіжці інформації за допомогою вірусів. Володар неліцензійного ПЗ не отримує технічної підтримки, своєчасних оновлень, що надаються компаніями-розробниками.

3. DDoS-атаки. Distributed-Denial-of-Service - «розподілена відмова від обслуговування» - це потік помилкових запитів від сотень тисяч географічно розподілених хостів, які блокують обраний ресурс одним з двох шляхів.

Перший шлях - це пряма атака на канал зв'язку. Другий - атака безпосередньо на сервер ресурсу. Зазвичай подібні атаки використовуються в ході конкурентної боротьби, шантажу компаній або для відвернення уваги системних адміністраторів від деяких протиправних дій.

4. Комп'ютерні віруси. Одна з найнебезпечніших на сьогоднішній день загроз інформаційній безпеці. Це можна пояснити появою нових каналів проникнення вірусів. На першому місці як і раніше залишається електронна пошта, але, як показує практика, віруси здатні проникати і через програми обміну повідомленнями, такі як ICQ та інші. Збільшилася і кількість об'єктів для можливих вірусних атак. Якщо раніше атакам піддавалися в основному сервери стандартних веб-служб, то сьогодні віруси здатні впливати і на міжмережеві екрани, комутатори, мобільні пристрої, маршрутизатори. Останнім часом особливо активні стали так звані віруси-шифрувальники.

5. Загрози з боку співвласників бізнесу (легальних користувачів інформації фірми). Такі витоки інформації фахівці називають інсайдерськими.

6. Законодавство. Державні органи наділені правом конфіскувати в ході перевірок обладнання та носії інформації, що завдає збитків компанії [1].

До методів захисту інформації слід віднести:

фізичні засоби захисту інформації (обмеження або повну заборону доступу сторонніх осіб на територію);

базові засоби захисту електронної інформації (численні антивірусні програми, а також системи фільтрації електронної пошти);

використання анти-DDoS (послугу анти-DDoS, пропоновані програмістами);

резервне копіювання даних (особливо актуальною стала послуга віддаленого зберігання різної інформації в «хмарі» дата-центрів);

план аварійного відновлення даних (в ньому обов'язково повинна бути передбачена можливість введення аварійного режиму роботи на період збою, а також всі дії, які повинні бути зроблені після відновлення даних. Сам процес відновлення слід максимально відпрацювати з урахуванням всіх змін системи;

шифрування даних при передачі інформації в електронному форматі (end-to-end protection) [1,2].

Визначення життєвого циклу інформаційної безпеки підприємства, дослідження основних рівнів інформаційної безпеки підприємства є також важливими аспектами її забезпечення в сучасних умовах їх господарювання.

**Список литературы**

1. Информационная безопасность предприятия: ключевые угрозы и средства защиты [Інтернет]. Доступно: https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html.

2. Грошева Е.К., Невмержицький И.П., “Информационная безопасность: современные реали”, *Международный научный электронный журнал «Бизнес-образование в экономике знаний»*, № 3, с. 35–37, 2017.