1. Основні поняття інформаційної безпеки

Інформаційна безпека — розділ інформатики, що вивчає закономірності забезпечення захисту інформаційних ресурсів фізичних осіб, підприємств, організацій, державних установ тощо від втрати, порушення функціонування, пошкодження, спотворення, несанкціонованого копіювання та використання.

Інформаційна безпека базується на таких принципах: **доступність, конфіденційність, цілісність.**

Основні загрози інформаційні безпеці:

- Знищення та спотворення даних;
- отримання доступу до конфіденційних даних;
- пошкодження пристроїв ІС;
- отримання прав на виконання певних дій;
- отримання доступу до виконання фінансових операцій;
- отримання повного доступу до керування ІС.

Загрози безпеці інформаційної системи (ІС) класифікують за такими принципами:

- За обсягом завданих збітків (*нешкідливі, шкідливі, дуже шкідливі*);
- За метою (*зловмисні, випадкові*);
- За місцем виникнення (з*овнішні; внутрішні);*
- За походженням (п*ридодні; техногенні; антропогенні*).

Етичні й правові основи інформаційної безпеки

Засоби і методи підтримки інформаційної безпеки мають різне призначення.

Програмні засоби — захист від вірусів, ідентифікація користувачів тощо.
Технічні засоби — захист від несанкціонованого доступу, від пошкодження ІС тощо.
Адміністративні методи — регламентація порядку взаємодії користувачів із ІС.
Морально-етичні засоби — норми поведінки осіб в інформаційному просторі.
Правові методи — правила користування інформацією та відповідальність за їхнє порушення.

Етичні норми передбачають, що користувачі комп'ютерів не використовують комп'ютерну техніку та програмне забезпечення для завдання шкоди іншим людям, не порушують авторських прав.

Правові основи захисту даних базуються на правових актах, що утверджують права і свободи людини та якими встановлено відповідальність

за злочини в галузі інформаційної безпеки. В Україні прийнято низку законів та постанов щодо забезпечення інформаційної безпеки: **«Про захист інформації в інформаційно—телекомунікаційних системах», «Про державну таємницю», «Про захист персональних даних», «Про авторське право та суміжні права»** та ін.
Незаконне втручання в роботу комп'ютерів, комп'ютерних мереж та розповсюдження вірусів тягне за собою кримінальну відповідальність (**ст. 361 Кримінального кодексу України**).

Організаційні принципи захисту даних:

- захист від втрати даних унаслідок стихійних явищ, збоїв у роботи електромереж, некомпететності працввників тощо;
- захист від умисного пошкодження комп'ютерного та мережевого обладнання, викрадення даних безпосередньо з пристроїв;
- захист від викрадення даних.

Авторське право

Інтелектуальна власність — це власність на результати інтелектуальної або творчої діяльності.

Об'єктами інтелектуальної власності є програмні продукти, бази даних, твори літератури, науки, мистецтва тощо.

Авторське право — це сукупність установлених і гарантованих державою прав автора щодо створення або використання об'єктів творчої діяльності.

Нормативні акти, що регулюють захист інтелектуальної власності:

- Закон України «Про авторське право і суміжні права», який набув чинності 23 лютого 1994 р.;
- Цивільний кодекс України (глава 36), ухвалений 16 січня 2003 р.

Знак охорони авторського права — знак © (перша літера англ. слова **Copyright**), що закріплює найменування власників авторського права та рік першої публікації твору.

Плагіат (лат. plagium — викрадення) — привласнення авторства на чужий твір науки, літератури, мистецтва або на чуже відкриття, винахід, а також використання в своїх працях чужого твору без посилання на автора.

Використовуючи матеріали з Інтернету — копіюючи їх на носії даних, вставляючи в презентації чи текстові документи, потрібно дотримуватися певних правил, щоб не порушити закон про захист авторських прав:

1. Запитувати дозвіл на використання матеріалів у автора. Це можна зробити, надіславши листа автору, якщо його ім'я або контактні дані вказано на сайті.

2. Використовуючи матеріали, отримані з Інтернету, обов'язково вказувати адресу сайту, звідки вони були скопійовані.

3. Не розповсюджувати чужі твори без дозволу автора.

Запобігання Інтернет-загрозам

Брандмауер — це технічний пристрій (маршрутизатор, роутер тощо) або програмний засіб для контролю даних, що надходять до комп'ютера через мережу.

Зверни увагу!

Брандмауери не запобігають витоку персональної інформації та завантаженню користувачами вірусів.

Щоб увімкнути і налаштувати вбудований брандмауер Windows , слід виконати: **Пуск → Панель керування → брандмауер Windows.**

Браузери мають вбудовані засоби захисту від Інтернет—загроз. Браузер Google Chrom:

• попереджає про відкриття сайта із загрозою фішингу або шкідливих програм;
• ізольовано відкриває веб—сторінки, що в разі загрози приводить до закриття лише однієї шкідливої сторінки;
• дозволяє відмінити збереження конфіденційних даних;
• надає можливість налаштувати показ спливаючих вікон.

Основні типи шкідливих програм та загроз при роботі в Інтернеті

Хробаки (черви) — програми, які самостійно поширюються мережею, не «інфікуючи» інші файли.

Трояни — програми, що поширюються під виглядом нешкідливих програм та виконують несанкціоновані дії: викрадають інформацію (паролі, рахунки тощо), передають її злочинцям через Інтернет, самостійно відкривають сайти для зміни рейтингів, хакерських атак тощо.

Скрипт-віруси — програми, що потрапляють на комп'ютер через електронну пошту, маскуючись під документи.

Дропери — виконувані файли, які самі не є вірусами, але призначені для встановлення шкідливих програм.

Боти — програми, які дають можливість зловмиснику таємно керувати вашим комп'ютером.

Шпигунські й рекламні програми — це програми, що зазвичай встановлюються на комп'ютер разом із безкоштовними програмами й збирають конфіденційну інформацію або демонструють нав'язливу рекламу.

Фішинг — вид Інтернет—шахрайства: виманювання конфіденційної інформації через підробні сайти, які копіюють сайти відомих банків, інтернет-магазинів тощо, або за допомогою спаму.

Спам — це небажана пошта переважно рекламного характеру. Спами можуть містити посилання на небезпечні сайти, заманливі пропозиції перерахувати гроші на певні рахунки тощо.

Зверни увагу!

Найнадійніший спосіб захисту від спаму — не дати можливість роботам упізнати вашу електронну адресу.

Програмні засоби боротьби зі спамом — спамфільтри — можуть бути складовими антивірусних програм або послугою поштових серверів. Багато поштових серверів дозволяють користувачам задавати власні фільтри й правила обробки поштових надходжень на основі набору символів з адреси відправника тощо.