Урок №3. **Тема.** **Загрози безпеці інформації в автоматизованих системах. Основні джерела і шляхи реалізації загроз безпеки та каналів проникнення і несанкціонованого доступу до відомостей та програмного коду**

Повторення основних класифікацій загроз інформаційній безпеці.



**V. Вивчення нового матеріалу**

 *6*. **Шляхи поширення загроз (людський чинник):**

1. **Глобальна мережа Інтернет** унікальна тим, що не є чиєюсь власністю і не має територіальних меж. Це багато в чому сприяє розвитку численних веб-ресурсів і обміну інформацією. Зараз будь-яка людина може дістати доступ до даних, що зберігаються в Інтернеті, або створити свій власний веб-ресурс. Ці особливості глобальної мережі надають зловмисникам можливість скоєння злочинів в Інтернеті, утрудняючи їх виявлення і покарання.
2. **Інтранет** – це внутрішня мережа, спеціально розроблена для управління інформацією усередині компанії або приватної домашньої мережі. Інтранет є єдиним простором для зберігання, обміну і доступу до інформації для всіх комп'ютерів мережі. Тому, якщо який-небудь із комп'ютерів мережі заражений, решту комп'ютерів піддано величезному ризику зараження. Щоб уникнути виникнення таких ситуацій, необхідно захищати не лише периметр мережі, але й кожний окремий комп'ютер.
3. **Електронна пошта**. Наявність поштових застосунків практично на кожному комп'ютері і використання шкідливими програмами вмісту електронних адресних книг для виявлення нових жертв забезпечують сприятливі умови для розповсюдження шкідливих програм.
4. **Знімні носії інформації** — дискети, CD-диски, флеш-карти — широко використовують для зберігання і поширення інформації. При активуванні файлу знімного носія, що містить шкідливий код, є загроза пошкодити дані на вашому комп'ютері і розповсюдити вірус на інші носії інформації або комп'ютери мережі.

 *7*. **Шкідливі програми (malicious software або malware)** – це програми, які призначені для того, щоб чинити шкоду і використовувати ресурси комп’ютера, вибраного в якості мішені. Вони часто маскуються в легальних програмах або імітуються під них. У деяких випадках вони розповсюджуються самі по собі, переходячи по електронній пошті від одного комп’ютера до іншого, або через заражені файли і диски.

1. Першу групу складають ті програми, **що вимагають програм-носіїв**. До них, в основному, відносяться фрагменти програм, що не можуть існувати незалежно від програм-носіїв, у ролі яких можуть виступати деякі програмні додатки, утиліти, системні програми. В цю групу входять:

- люки;

- логічні бомби;

- троянські коні;

- віруси.

У другу групу входять програми, **що є незалежними**. До них відносяться окремі незалежні програми, які можуть плануватися і запускатися операційною системою. До цієї групи належать:

- черв’яки,

- зомбі;

- утиліти прихованого адміністрування;

- програми-крадії паролів;

- «intended»-віруси;

- конструктори вірусів;

- поліморфік-генератори.

**Крім того, небезпечні програми поділяються на такі, що:**

**- не відновлюють себе** (не розмножуються). До них відносяться фрагменти програм, які повинні активізуватися під час певних дій головної програми;

**- розмножуються** - фрагменти програм (віруси), або незалежні програми (черв’яки), що здатні під час запуску створювати одну або декілька копій самих себе. Ці копії пізніше також активізуються в цій самій або іншій операційній системі.

**Люк** – це прихована, недокументована точка входу в програмний модуль, яка дозволяє кожному, хто про неї знає, отримати доступ до програми в обхід звичайних процедур, призначених для забезпечення безпеки КС.

**Логічна бомба** – це код, що поміщається в деяку легальну програму. Він влаштований таким чином, що при певних умовах «вибухає». Умовою для включення логічної бомби може бути наявність або відсутність деяких файлів, певний день тижня або певна дата, а також запуск додатку певним користувачем.

**Троянський кінь** – це програма, яка виконує на доповнення до основних (проектних i документованих) додаткові, але не описані в документах, дії. Троянський кінь – це корисна, або така, що здається корисною, програма або процедура, в якій приховано код, здатний в разі спрацьовування виконати деяку небажану або шкідливу функцію.

**Черв'як** - це програма, яка розповсюджується через мережу і не залишає своєї копії на магнітному носії. Черв'як використовує механізм підтримки мережі для визначення вузла, який може бути заражений. Потім за допомогою тих самих механізмів передає своє тіло на цей вузол й або активізується, або чекає для цього певних сприятливих умов.

**Зомбі** - це програма, яка приховано під’єднується до інших підключених в Інтернет комп’ютерів, а потім використовує цей комп’ютер для запуску атак, що ускладнює відстеження шляхів до розробника програми-зомбі.

**Захоплювачі паролів** - це спеціально призначені програми для крадіжки паролів. Вони виводять на екран терміналу (один за одним) порожній екран, екран, який з'являється після катастрофи системи або сигналізує про закінчення сеансу роботи.

**До іntended-вірусів** відносяться програми, що на перший погляд є стовідсотковими вірусами, але не спроможні розмножуватися через помилки. Наприклад, вірус, що при інфікації «забуває» передбачити активізацію вірусу, що розмножується тільки один раз – із «авторської» копії. Інфікувавши якийсь файл, вони втрачають спроможність до подальшого розмноження. Частіше за все intended-віруси з’являються при неякісній перекомпіляції якогось вже існуючого вірусу, або через недостатнє знання мови програмування, або через незнання технічних тонкощів операційної системи.

**Конструктор вірусів -** це програма, що призначена для виготовлення нових комп’ютерних вірусів. Відомі конструктори вірусів для DOS, Windows і макровірусів. Вони дозволяють генерувати вихідні тексти вірусів (ASM-файли), об’єктні модулі і (або) безпосередньо інфікувати файли.

**Поліморфік-генератори**, як і конструктори вірусів, не є вірусами в буквальному значенні цього слова, оскільки в їхній алгоритм не закладаються функції розмноження, тобто відкриття, закриття і запису у файли, читання і запису секторів і т.д. Головною функцією подібного роду програм є шифрування тіла вірусу і генерація відповідного розшифровувача.

 *8.***Комп'ютерний вірус** ([англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) computer virus) — комп'ютерна програма, яка має здатність до прихованого самопоширення. Одночасно зі створенням власних копій [віруси можуть завдавати шкоди](https://uk.wikipedia.org/wiki/%D0%A8%D0%BA%D1%96%D0%B4%D0%BB%D0%B8%D0%B2%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B8%D0%B9_%D0%B7%D0%B0%D1%81%D1%96%D0%B1): знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність [операційної системи](https://uk.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) комп'ютера.

* 9.* ***Класифікація комп’ютерних вірусів***

 *10.* **Ознаки зараження вірусом**

* Зменшення вільної пам'яті.
* Уповільнення роботи комп'ютера.
* Затримки при виконанні програм.
* Незрозумілі зміни в файлах.
* Зміна дати модифікації файлів без причини.
* Незрозумілі помилки Write-protection.
* Помилки при інсталяції і запуску Windows.
* Відключення 32-розрядного допуску до диску.
* Неспроможність зберігати документи Word в інші каталоги, крім Template.
* Погана робота дисків.
* Файли невідомого походження.

Ранні ознаки зараження дуже тяжко виявити, але коли вірус переходить в **активну фазу, тоді легко помітити такі зміни:**

* зникнення файлів;
* форматування HDD;
* неспроможність завантажити комп'ютер;
* неспроможність завантажити файли;
* незрозумілі системні повідомлення, звукові ефекти і т. д.

 *11.* З розвитком інтернет-технологій часто люди можуть стати жертвами інтернет-шахраїв. Їхня анонімність та вигадливість, а також довірливість користувачів підживлюють цей «бізнес».

* Шахрайства, пов'язані з покупками через мережу Інтернет.
* Шахрайства, пов'язані з продажами через мережу Інтернет.
* Інтернет-жебрацтво.
* Ви виграли цінний приз!
* Шахрайство з надзвичайною ситуацією/рідними.
* Фішинг.
* Скімінг.

 *12*. **Спам-розсилки**

**Спам** — масове розсилання [кореспонденції](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D1%80%D0%B5%D1%81%D0%BF%D0%BE%D0%BD%D0%B4%D0%B5%D0%BD%D1%86%D1%96%D1%8F) рекламного чи іншого характеру людям, які не висловили бажання її одержувати.

Спеціальні програми, спам-боти, ходять по різних сайтах, зчитують, де це можливо, e-mail адреси, які викладені у відкритому вигляді і заносять до спеціальних баз. Потім по цих базах листи і розсилаються.

### Види спаму:

### Реклама

### Нігерійські листи

### Фішинг

* Розсилання листів [релігійного](https://uk.wikipedia.org/wiki/%D0%A0%D0%B5%D0%BB%D1%96%D0%B3%D1%96%D1%8F) змісту.
* Масове розсилання для виведення поштової системи з ладу ([відмова сервісу](https://uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0)).
* Масове розсилання від імені іншої особи, з метою викликати до неї негативне ставлення.
* Масове розсилання листів, що містять [комп'ютерні віруси](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81) (для їхнього початкового поширення).

 *13.* Найнадійніший засіб боротьби зі спамом — не дозволити спамерам роздобути вашу електронну адресу. Це важке завдання, але деякі запобіжні заходи все ж варто вжити.

* Не варто без необхідності публікувати адресу електронної пошти на веб-сайтах чи в групах Usenet.
* Не потрібно реєструватися на підозрілих сайтах. Якщо якийсь корисний сайт вимагає реєстрації, можна вказати спеціально для цього створену адресу.
* Ніколи не відповідати на спам і не переходити за посиланнями, які містяться в ньому. Цим ви тільки підтвердите, що користуєтеся своєю електронною адресою й будете отримувати ще більше спаму.
* Вибираючи собі ім'я електронної пошти варто, за можливості, обирати довге й незручне для вгадування ім'я.

 *14*. **Ботнет (англ. *Botne* від robot і network)—** це мережа пов'язаних між собою вірусом комп'ютерів, які управляються зловмисниками з командного центру.

 **Основні можливості ботнетів:**

* перехоплення даних, які користувач вводить (логіни, паролі, дані кредитних карт) і передача їх у командний центр;
* атаки на конкретні інтернет-ресурси. Залучені в ботнет комп'ютери відправляють по команді постійні запити на певний сайт, внаслідок чого той, не витримуючи такого навантаження, відключається;
* розсилка спаму. Більше 80% світового спаму розсилається з зомбі-комп'ютерів.

 *15.* **Основні ознаки зараження комп'ютера і належності до машин ботнету.**

* Програмне забезпечення посилено звертається до Інтернету, намагаючись встановити зв'язок з провайдером в будь-який час, коли комп'ютер включений.
* На порядок збільшується мережний трафік.
* В системних процесах з'являється багато нових, яких раніше не було, причому нові процеси маскуються під системні (тобто мають схожі з ними імена).

 *16*. **Поширені загрози від мережі ботнетів:**

* DDoS-атаки;
* спам-розсилки;
* збільшення клік-лічильників;
* пошуковий спам;
* збирання секретної інформації.

 *17*. **Атака на відмову в обслуговуванні, (англ. DoS attack, DDoS attack, (Distributed) Denial-of-service attack)** — напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

 *18.* Існують прості **фінансові** **правила поведінки в Інтернеті**, завдяки яким Ви і Ваші гроші будете захищені від кібератак.

1. Запам'ятайте, що банк або інша фінансова установа ніколи не просить клієнтів передавати електронною поштою такі дані, як номер і термін дії картки, ПІН-код тощо.
2. Не відкривайте додатки до листів, отриманих від невідомих Вам відправників.
3. Нікому не повідомляйте свої логіни і паролі до аккаунтів у платіжних системах, ПІН-коди та іншу інформацію, яка стосується Ваших рахунків і банківських карток.
4. Обережно використовуйте картку під час розрахунків в Інтернеті.
5. Купуйте товари та послуги на тих сайтах, які вказують свої контактні дані. У разі необхідності, ви повинні знати, куди звернутися з питанням або претензією.
6. Для розрахунків в Інтернеті краще завести спеціальну картку і не зберігати на ній великі суми.
7. Регулярно перевіряйте стан рахунку і залишок на ньому. Якщо виявите зникнення коштів, негайно зв'язуйтеся з банком і блокуйте рахунок.
8. Також намагайтеся не зберігати конфіденційні дані на жорсткому диску в незашифрованому вигляді і регулярно оновлюйте антивірусну базу свого комп'ютера.

 *19.* **Крадіжка особистості (Identity Theft)** – злочин, при якому незаконно використовуються персональні дані людини для отриманні матеріальної вигоди.

* ***Практичне завдання*** *( 22)*

Групова робота (2-3 учнів)

* 1. Визначити основні характеристики типу вірусів.
	2. Підготувати коротке повідомлення (1-2 хв);
	3. Результати оформити в Google-документ – створити одну спільну таблицю (максимум 2 ст.).
	4. Надати доступ вчителеві.
* 1 група – люки
* 2 група – логічні бомби
* 3 група – троянські коні
* 4 група – черв’яки
* 5 група – зомбі
* 6 група – утиліти прихованого адміністрування

**VII. Підведення підсумків уроку**

* ***Бесіда за питаннями*** *( 23)*
1. Назвіть основні шляхи поширення загроз.
2. Шкідливі програми поділяються на два великих типи…
3. Комп’ютерний вірус - це…
4. Які основні види інтернет-шахрайства ви знаєте?
5. Що таке спам?
6. Поясніть значення слова «фішинг».

**VIII. Домашнє завдання**

 *24.*Створити карту фінансових правил поведінки в Інтернеті, використовуючи Google-малюнки.

Надати доступ учителеві.