«___»_____ 20___ року

Урок №4. **Технічні засоби добування інформації. Програмні засоби добування інформації**

Технічні і програмні засоби добування необхідної інформації - це подолання системи захисту, обмеження або заборона доступу до них посадових осіб, дезорганізації роботи технічних засобів, вивід з ладу комунікаційних і комп'ютерних мереж, усього високотехнологічного забезпечення функціонування системи управління.

Технічні засоби добування інформації

- Технічні засоби добування інформації.
- Добування інформації без порушення кордонів контрольованої зони.
- Передача інформації практично в реальному масштабі часу в будь-яку точку земної кулі.
- Аналіз і обробка інформації в обсязі і за час, недосяжний людині.
- Консервація і необмежений час зберігання видобутої інформації.

Програмні засоби добування інформації

- Комп'ютерний вірус
- «Троянський кінь»
- «Нейтралізатори текстових програм» - це програми, що забезпечують невиявлення випадкових і навмисних хиб програмного забезпечення.
- Засоби впровадження КВ і ЛБ в інформаційні ресурси автоматизованої системи і керування ними на відстані.
- Засоби придушення інформаційного обміну в телекомунікаційних мережах, фальсифікації інформації в каналах.
- Логічна бомба.

Хробаки – це один із різновидів шкідливих вірусів, що розмножуються та псують дані, збережені на комп’ютері.

- Використовують так звані «дірки» (уразливості) у програмному забезпеченні операційних систем.
- Розповсюджуються найчастіше через файли, вкладені в електронні листи.
- Проникають на комп'ютер-жертву без участі користувача.

<u>Різновиди:</u>

- Мережні хробаки
- Поштові хробаки
- IRC-хробаки
- P2P-хробаки
- IM-хробаки

<u>Життєвий цикл:</u>

- Проникнення в систему
- Активація
- Пошук «жертв»
- Підготовка копій

- Поширення копій

Логічна бомба (англ. *Logic bomb*) — програма, яка запускається за певних часових або інформаційних умов для здійснення зловмисних дій (як правило, несанкціонованого доступу до інформації, спотворення або знищення даних).

- Код, що поміщається в легальну програму.
- Мета - несанкціонований доступ до інформації, спотворення або знищення даних.
- Будучи активною, «Логічна Бомба» запускає невелику програму, яка має шкідливий вплив на роботу комп'ютерної системи чи мережі.

Троян (троянський кінь) — тип шкідливих програм, що дозволяє здійснювати схований, несанкціонований доступ до інформаційних ресурсів для добування інформації.

Попадає в систему разом з вірусом або хробаком

Виявити «троянського коня» дуже важко, оскільки сучасні програми складаються з тисяч і навіть мільйонів команд і мають складну структуру.

Можливість зі збереженням працездатності програми виконати додаткові, незадокументовані функції, наприклад, переслати інформацію (зокрема паролі), що зберігається на комп'ютері.

До даної групи шкідливих програм відносять:

- програми-вандали;
- «дроппери» вірусів;
- «злі жарти»;
- деякі види програм-люків;
- програми вгадування паролів;
- програми прихованого адміністрування.

Утиліта прихованого адміністрування (backdoor).

- Є досить могутніми утилітами віддаленого адміністрування комп'ютерів у мережі.
- Уражені комп'ютери виявляються відкритими для злочинних дій хакерів.
- Дозволяють робити з комп'ютером усе, що в них заклав їх автор: приймати і відсилати файли, запускати і знищувати їх, виводити повідомлення, стирати інформацію, перевантажувати комп'ютер і т.д.
- Використовують для виявлення і передачі конфіденційної інформації, для запуску вірусів, знищення даних.
- Під час запуску утиліта прихованого адміністрування встановлює себе в системі і потім стежить за нею, при цьому користувачу не видається ніяких повідомлень про дії такого трояна в системі.
- Можна віднести до групи троянських коней.

«Жадібні» програми (greedy program) – це програми, що намагаються монополізувати який-небудь ресурс, не даючи іншим програмам можливості використовувати його.

Захоплювачі паролів - це спеціально призначені програми для крадіжки паролів.

Ознаки зараження ПК вірусом або шкідливим програмним забезпеченням.

- Зменшення вільної пам'яті
- Зміна дати модифікації файлів без причини
- Незрозумілі зміни в файлах
- Файли невідомого походження
- Помилки про інсталяції і запуску Windows
- Затримки при виконанні програм
- Уповільнення роботи комп'ютера

Правила захисту Вашого ПК

- **Використовуйте антивірусну програму та постійно оновлюйте її** Майже відразу після появи WannaCry основні антивірусні постачальники випустили оновлення для захисту своїх користувачів.
- **Не натискайте на посилання або не відкривайте вкладення, які надійшли з невідомих для вас електронних** адрес Одне з найголовніших джерел шкідливих програм – електронні листи від шахраїв. Навіть коли вони потрапляють вам у папку «Спам», то здійснюють фішинг (пошук інформації про вас) на вашому комп’ютері.
- **Миттєво закривайте сайти, які відкрилися на комп’ютері без вашої згоди** На веб-браузері, яким ви користуєтеся, має спрацьовувати блокування. Це дозволяє не показувати потенційно небезпечні оголошення на екрані. Google Chrome, Firefox і Microsoft Edge мають вбудовані блокувальники.
- **Блокуйте спливаючі вікна, скачування та відкривання дивних файлів** Ніколи не натискайте на таких сайтах ні на що, крім «хрестика» закрити. Будь-який клік може призвести до завантаження зловмисного програмного забезпечення на комп’ютер.
- **Регулярно створюйте резервні копії ваших важливих файлів.** Це можна робити на зовнішньому диску або ж, якщо у вашій команії є служба віддаленого зберігання.
- **Блокуйте автоматичний запуск.** Багато вірусів прикріплюють себе до диска і автоматично встановлюються, коли такий носій підключений до системи. Як результат під’єднання будь-якого мережевого диска, зовнішнього жорсткого диска і навіть флешки може привести до автоматичного поширенню таких загроз.
- Розумний серфінг в мережі.
- **Звертайте увагу на сповіщення Windows SmartScreen.** Не запускайте невідомі програми, завантажені з Інтернету. Дуже ймовірно, що нерозпізнані програми є небезпечними. Коли завантажуєте з Інтернету та запускаєте програму, фільтр SmartScreen перевіряє її репутацію, щоб попередити вас, якщо вона невідома або може виявитися зловмисною.
- **Використовуйте брандмауер.** Брандмауер Windows або інша програма-брандмауер сповіщає про підозрілі дії, якщо вірус або хробак намагається підключитися до комп’ютера. Брандмауер може також блокувати

віруси, хробаки та дії хакерів, які мають на меті завантажити на комп’ютер потенційно небезпечні програми.

- **Перед використанням чужих носіїв інформації, обов’язково перевірте їх**

Перелік заходів із безпеки для Windows

Центр підтримки. Відвідайте Центр підтримки та переконайтеся, що брандмауер активовано, програму захисту від зловмисного програмного забезпечення оновлено, а ПК настроєно на автоматичну інсталяцію оновлень.

Захисник Windows. Скористайтеся програмою «Захисник Windows», щоб уникнути інсталяції вірусів, шпигунського та іншого зловмисного або небажаного програмного забезпечення на ПК без вашого відома.

Windows SmartScreen. Засіб Windows SmartScreen допомагає захистити ПК, попереджуючи вас перед запуском нерозпізнаних програм і файлів, завантажених з Інтернету.

Служба захисту користувачів. Служба захисту користувачів запитує дозвіл на інсталяцію на ПК програмного забезпечення або відкривання певних типів програм, які можуть зашкодити комп’ютеру чи зробити його вразливим до інших загроз системі безпеки.

Банк файлів. Банк файлів використовується для автоматичного регулярного резервного копіювання особистих файлів, як-от фотографій, документів і музики. У разі відмови устаткування ПК можна відновити будь-яку версію найважливіших файлів.

Windows Update. Використовуйте службу Windows Update для автоматичного завантаження та інсталяції найновіших оновлень для ПК.

Брандмауер Windows. Активуйте Брандмауер Windows, щоб запобігти доступу хакерів і програм, створених зловмисниками, наприклад, вірусів, до ПК через Інтернет.

Смартфон чи планшет, яким ви користуєтеся для оплати товарів у Інтернеті, придбання квитків, чи навіть просто ігор — дуже зручний інструмент для шахраїв, аби виманити ваші особисті дані і скористатися ними у власних незаконних цілях. Якщо, звісно, ви не дотримуєтесь певних простих правил.

- Не проводьте платіжні операції у відкритій, незахищеній мережі Wi-Fi.
- Завантажте офіційний застосунок вашого банку і кожного разу перевіряйте — чи ви на потрібному сайті.
- Відключіть автоматичний вхід в обліковий запис на сайті чи мобільному застосунку. Декідька хвилин на введення логіну-паролю – але значно вищий ступінь захисту.
- Якщо є можливість, встановіть застосунок мобільної безпеки, що сповіщатиме про підозрілу діяльність.
- Не пересилайте платіжні дані текстовими повідомленнями.
- Не розголошуйте пароль і номер картки.
- Обов'язково повідомте банк при втраті чи зміні мобільного номеру для оновлення інформації.

Ознаки шкідливого ПЗ на смартфоні

- Надмірний нагрів.

- Зниження продуктивності.
- Періодично на смартфоні спливає реклама з пропозицією щось купити або десь зареєструватися.
- Підвищена витрата заряду акумуляторної батареї.
- Поява підозрілих іконок або невідомих ярликів на робочому столі.
- Спонтанні презавантаження.
- Збільшений інтернет-трафік.

Правила захисту Вашого смартфону

- Встановлюйте застосунки тільки з перевірених джерел.
- Відключіть автоматичний вхід в обліковий запис на сайті чи мобільному застосунку.
- Не пересилайте платіжні дані текстовими повідомленнями.
- Встановіть застосунок мобільної безпеки.
- Не натискайте на підозрілі вкладення чи посилання від неперевірених контактів.
- Після здійснення платежу – виходьте з облікового запису.
- Не користуйтесь незахищеним, відкритими Wi-Fi.
- Зробіть резервні копії своїх даних.
- Завжди читайте список необхідних додаткам дозволів.