**Міністерство освіти та науки України**

**Київський національний торговельно - економічний університет**

**Факультет інформаційних технологій**

**Кафедра інженерії програмного забезпечення та кібербезпеки**

**ПРАКТИЧНА РОБОТА № 01**

**З ДИСЦИПЛІНИ**

**«Безпека інформаційних систем»**

**НА ТЕМУ:**

ПОБУДОВА МОДЕЛІ ЗАГРОЗ БЕЗПЕКИ ІНФОРМАЦІЇ В ІС

**Виконала:** студентка ФІТ

Групи 4 курсу 3

Авєріна Наталія Ігорівна

**Викладач:** Лахно Валерiй Анатолiйович

Київ 2023

**Практична робота №01**

Тема: «Побудова моделі загроз безпеки інформації в ІС».

Мета: навчитися будувати моделі загроз безпеки інформації в ІС.

Модель загальних загроз:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Назва загрози | Опис загрози та можливі наслідки реалізації | Об’єкти загрози | Суб’єкт загрози | Можлива атака | Дестабілізуючі фактори | Вразливість, що може використовуватись | Тип загрози |
| Фізичне пошкодження обладнання | Наприклад, пожежа, затоплення, землетрус або інші природні катастрофи, які можуть призвести до фізичного знищення або пошкодження обладнання ІКС. | Технічні засоби, носії інформації. | Зовнішнє середовище. | - | Недотримання правил протипожежної безпеки, несправності електричної проводки, перенавантаження електромережі, невідповідність інженерних характеристик будівлі, несправність інженерних конструкцій. | Відсутність системи пожежогасіння, відсутність географічно розподіленої системи резервування даних, невідповідність умовам розміщення технічних засобів. | Ц, Д, С |
| Втрата електропостачання | Відсутність електроенергії або несправність живлення може призвести до припинення роботи системи або втрати даних. | Електромережа, електрообладнання, електропідстанції. | Природні чинники (наприклад, природні лиха, такі як шторми або землетруси), технічні несправності, людський фактор (наприклад, неправильна експлуатація обладнання). | Вплив на електромережу або електрообладнання з метою призупинення електропостачання. | Природні катастрофи, технічні несправності, неправильне планування та управління енергосистемою. | Недостатній захист електромережі та електрообладнання від негативного впливу. | Ц, Д, С |
| Людський фактор | Внутрішні загрози, пов'язані з недбалістю персоналу, несанкціонованим доступом, витоками інформації через соціальні інженерні атаки. | Персонал організації, користувачі інформаційних систем. | Робітники, адміністратори, користувачі. | - | Недостатня освіта та навчання персоналу з питань безпеки, недостатній контроль та аудит в діяльності персоналу. | Відсутність свідомості про правила безпеки серед персоналу, відсутність систем аудиту та моніторингу дій персоналу. | К, Ц, Д, С |

Модель мережевих загроз:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Назва загрози | Опис загрози та можливі наслідки реалізації | Об’єкти загрози | Суб’єкт загрози | Можлива атака | Дестабілізуючі фактори | Вразливість, що може використовуватись | Тип загрози |
| Перехоплення даних (Data Interception) | Атака на перехоплення інформації під час її транспортування через мережу в наслідку якої несанкціонований доступ до конфіденційної інформації, можливість читання чутливих даних. | Передані дані, комунікаційні канали. | Хакер, зловмисник, прослуховувач. | Захоплення пакетів, використання "packet sniffers". | Слабке шифрування, відкриті мережеві точки. | Відсутність або слабке шифрування даних. | К, Ц, С |
| Несанкціонований доступ (Unauthorized Access) | Спроба отримання доступу до мережевих ресурсів без дозволу. Результатом чого можуть бути модифікація чи видалення даних. | Мережеві ресурси, системні дані. | Зловмисник, хакер. | Перехоплення аутентифікаційних даних, використання слабких паролів. | Слабка аутентифікація, відкриті порти. | Несправна аутентифікація та авторизація. | К, Ц, Д, С |
| Внедрення зловмисного програмного забезпечення (Malware Injection) | Введення в мережу шкідливого програмного забезпечення для завдання шкоди або отримання несанкціонованого доступу. | Мережеві точки, файли, додатки. | Зловмисник, хакер. | Введення в систему вірусів, троянів, черв'яків. | Відсутність антивірусного програмного забезпечення, відкриті порти. | Недостатній захист від шкідливого програмного забезпечення. | К, Ц, Д, С |
| Відмова в обслуговуванні (DoS) | Завдання перевантаження або переповнення мережевих ресурсів з метою призупинення їх нормального функціонування. | Сервери, комунікаційні канали. | Зловмисник, хакер | Використання багатьох запитів або переповнення даними. | Відсутність систем захисту від DoS-атак, відкриті ресурси. | Недостатня пропускна здатність, слабка система захисту. | Д, С |

Модель загроз прикладного ПЗ

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Назва загрози | Опис загрози та можливі наслідки реалізації | Об’єкти загрози | Суб’єкт загрози | Можлива атака | Дестабілізуючі фактори | Вразливість, що може використовуватись | Тип загрози |
| Помилка, збій та відмова прикладного ПЗ | Помилка, збій або відмова прикладного програмного забезпечення (ПЗ) може виникнути внаслідок програмних помилок, несправностей апаратного забезпечення, неправильної конфігурації, атак або інших небезпечних сценаріїв. Відмова прикладного ПЗ може призвести до недоступності сервісу, втрати або пошкодження даних, порушення конфіденційності, порушення цілісності системи і негативно вплинути на продуктивність користувачів. | Прикладне та системне ПЗ, слабко- та сильно- пов’язані об’єкти, обчислювальні ресурси. | Прикладне та системне ПЗ, зовнішнє середовище, адміністратори, користувачі, зловмисники, хакери. | Вірусна атака, DoS. | Використання неліцензійного та нерегламентованого ПЗ, помилки при інсталяції та конфігуруванні ПЗ, недостатні періоди тестування ПЗ перед впровадженням у промислову експлуатацію. | Вразливість у програмному коді, відсутність або недостатність антивірусного захисту, порушення процедур інсталяції та використання ПЗ. | К, Ц, Д, С |

Модель загроз ОС

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Назва загрози | Опис загрози та можливі наслідки реалізації | Об’єкти загрози | Суб’єкт загрози | Можлива атака | Дестабілізуючі фактори | Вразливість, що може використовуватись | Тип загрози |
| Помилка, збій та відмова системного ПЗ | Помилки та відмови системного ПЗ, що можуть виникати внаслідок неправильних налаштувань ОС, помилок розробників ОС, невідповідності системним вимогам тощо (ненавмисна загроза). Це може призводити до втрати чи перекручення даних, відмови прикладного ПЗ та виходу з ладу компонентів надмірного використання обчислювальних ресурсів. | Прикладне та системне ПЗ, слабко- та сильно- пов’язані об’єкти, обчислювальні ресурси. | Системне ПЗ, зовнішнє середовище, адміністратори, користувачі. | Вірусна атака, застосування шкідливого ПЗ. | Використання неліцензійного та нерегламентованого ПЗ, помилки при інсталяції та конфігуруванні ОС. | Вразливість у програмному коді, відсутність або недостатність антивірусного захисту, порушення процедур інсталяції та використання ОС, відсутність правил розповсюдження і використання ПЗ. | К, Ц, Д, С |