**Заняття 4. Лекція 6. Модель загроз для інформації.**

**Вступ.**

**Питання 1. Канали витоку інформації як джерело виникнення загроз.**

**Питання 2. Процес створення моделі загроз інформації.**

**2.1 Перелік загроз з визначенням порушень властивостей інформації та ІТС**

**2.2 Модель загроз з визначенням рівня ризиків та збитків.**

**2.2.1 Модель загроз з розрахунком сумарного рівня ризиків та збитків.**

**2.3 Варіант моделі загроз для розподілених обчислювальних мереж.**

**Контрольні питання.**

**Вступ.**

Після проведення обстеження всіх середовищ ІТС необхідно визначити всі можливі потенційні загрози.

Походження загроз може бути випадковим і навмисним.

Випадкове походження обумовлюється спонтанними і не залежними від волі людей обставинами, що виникають в ІТС в процесі її функціонування. Найбільш відомими випадковими загрозами є стихійні лиха, відмови, збої, помилки та побічні впливи.

Сутність цих загроз (окрім стихійних лих, сутність яких незрозуміла) визначається таким чином:

- відмова - порушення працездатності системи, що призводить до неможливості виконання нею основних своїх функцій;

- збій - тимчасове порушення працездатності системи, наслідком чого може бути неправильне виконання у цей момент своїх функцій;

- помилка - неправильне виконання системою своїх функцій, що відбувається внаслідок її специфічного стану;

- побічний вплив - негативний вплив на систему, який чиниться будь-якими явищами, що відбуваються всередині системи або у зовнішньому середовищі.

Навмисне походження загроз обумовлюється зловмисними діями людей.

Передумови появи загроз можуть бути об'єктивними та суб'єктивними.

Об'єктивні передумови можуть бути спричинені кількісною або якісною недостатністю елементів системи тощо.

До суб'єктивних передумов відносяться різновиди людської діяльності: іноземна розвідка, промислове шпигунство, злочинні дії, неякісна робота персоналу ІТС.

Перераховані різновиди передумов інтерпретуються таким чином:

- кількісна недостатність - фізична нестача одного або декількох елементів системи, що викликає порушення технологічного процесу обробки даних і / або перевантаження наявних елементів.

- якісна недостатність - недосконалість конструкції (організації) елементів системи, в силу цього можуть з'являтися можливості випадкового або навмисного негативного впливу на оброблювану або збережену інформацію.

Джерело загрози - це безпосередній їх генератор або носій. Таким джерелом можуть бути люди, технічні засоби, моделі (алгоритми), а також - програми, технологічні схеми обробки, зовнішнє середовище.

Спробуємо тепер, спираючись на наведену системну класифікацію загроз безпеки інформації, визначити всю кількість загроз, потенційно можливих у сучасних ІТС. При цьому ми повинні врахувати не лише всі відомі загрози, але й ті загрози, що раніше не виявлялися, але потенційно можуть виникнути при застосуванні нових концепцій архітектурної побудови ІТС і технологічних схем обробки інформації.

**Питання 1.**

Всі можливі канали витоку інформації (КВІ) класифікуються за двома критеріями:

- наявність доступу до ІТС;

- стан функціонування ІТС.

За першим критерієм КВІ можуть бути розділені на такі, що:

- не вимагають доступу, тобто дозволяють отримувати необхідну інформацію дистанційно (наприклад, шляхом візуального спостереження через вікна приміщень ІТС),

- вимагають доступу в приміщення ІТС. У свою чергу, такі канали можуть не залишити слідів в ІТС (наприклад, візуальний перегляд зображень на екранах моніторів або документів на паперових носіях), а можуть і залишити ті чи інші сліди (наприклад, розкрадання документів або машинних носіїв інформації).

За другим критерієм КВІ можуть бути розділені на:

- потенційно існуючі незалежно від стану ІТС (наприклад, викрадати носії інформації можна незалежно від того, в робочому стані знаходяться засоби АС чи ні);

- існуючі тільки в робочому стані ІТС (наприклад, побічні електромагнітні випромінювання та наведення).

В результаті такої класифікації отримаємо 6 класів КВІ, які мають таку орієнтовну характеристику:

- 1-й клас - КВІ, які проявляються безвідносно до обробки інформації без доступу до елементів ІТС ( підслуховування розмов, а також провокування на розмови осіб, що мають відношення до ІТС, і використання зловмисником візуальних, оптичних та акустичних засобів);

- 2-й клас - КВІ, які проявляються у процесі обробки інформації без доступу до елементів ІТС (електромагнітні випромінювання різних пристроїв ІТС, апаратури та ліній зв'язку, паразитні наведення в ланцюгах харчування, телефонних мережах, системах теплопостачання, вентиляції тощо);

- 3-й клас - КВІ, які проявляються безвідносно до обробки інформації з доступом до елементів ІТС, але без зміни останніх (всілякі види копіювання носіїв інформації і документів, а також розкрадання виробничих відходів);

- 4-й клас - КВІ, які проявляються у процесі обробки інформації з доступом до елементів ІТС, але без зміни останніх (запам'ятовування та копіювання інформації в процесі обробки, використання програмних закладок тощо);

- 5-й клас - КВІ, які проявляються безвідносно до обробки інформації з доступом до елементів ІТС і зі зміною останніх (підміна та розкрадання носіїв інформації й апаратури, впровадження у програмне забезпечення шкідливих кодів, вірусів тощо);

- 6-й клас - КВІ, які проявляються у процесі обробки інформації з доступом до елементів ІТС і зі зміною останніх (незаконне підключення до апаратури та ліній зв'язку, а також зняття інформації з ліній живлення різних елементів ІТС).

**Питання 2.**

На підставі Акту обстеження та Моделі порушника політики безпеки СЗІ розробляє «Модель загроз для інформації в ІТС», яка затверджується керівником організації-власника (розпорядника) ІТС, та вноситься, за необхідності, до відповідних розділів Плану захисту та Технічного завдання на створення КСЗІ. Модель загроз має містити формалізований або неформалізований опис методів і засобів здійснення загроз для інформації, яка потребує захисту.

Модель загроз повинна визначити:

* перелік можливих типів загроз, класифікований за результатом впливу на інформацію, тобто на порушення яких її властивостей вони спрямовані (конфіденційності, цілісності або доступності інформації);
* перелік можливих способів реалізації загроз певного типу (способів атак) відносно різних інформаційних об’єктів ІТС у різному стані класифікований, наприклад, за такими ознаками, як компонент обчислювальної системи ІТС або програмний засіб, уразливості яких експлуатуються порушником, причини виникнення відповідної уразливості тощо.

Загрози для інформації, що обробляється в ІТС, залежать від характеристик ОС, апаратного складу, програмних засобів, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу.

Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно ІТС і повинні враховуватись у моделі загроз, наприклад:

* зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);
* збої та відмови у роботі технічних або програмних засобів (далі - ПЗ) ІТС;
* наслідки помилок під час проектування та розробки компонентів ІТС (технічних засобів, технології обробки інформації, ПЗ, засобів захисту, структур даних тощо);
* помилки персоналу (користувачів) ІТС під час експлуатації;
* навмисні дії (спроби) потенційних порушників.

Випадкові загрози суб’єктивної природи - це помилкові дії персоналу по неуважності, недбалості, незнанню тощо, але без навмисного наміру.

До них відносяться:

* дії, що призводять до відмови ІТС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв’язку, видалення даних, програм тощо);
* ненавмисне пошкодження носіїв інформації;
* неправомірна зміна режимів роботи ІТС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);
* неумисне зараження ПЗ комп’ютерними вірусами;
* невиконання вимог до організаційних заходів захисту чинних в ІТС розпорядчих документів;
* помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;
* будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;
* неправомірне впровадження та використання заборонених політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення тощо);
* наслідки некомпетентного застосування засобів захисту тощо.

Навмисні загрози суб’єктивної природи – це дії порушника, спрямовані на проникнення в систему та одержання можливості НСД до її ресурсів або дезорганізацію роботи ІТС та виведення її з ладу.

До них відносяться:

* порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації);
* порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, заземлення, охоронної сигналізації, кондиціонування тощо.);
* порушення режимів функціонування ІТС (обладнання і ПЗ);
* впровадження та використання комп’ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;
* використання (шантаж, підкуп тощо) з корисливою метою персоналу ІТС;
* крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);
* несанкціоноване копіювання носіїв інформації;
* читання залишкової інформації з оперативної пам’яті ЕОТ, зовнішніх накопичувачів;
* одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача;
* неправомірне підключення до каналів зв’язку, перехоплення даних, що передаються, аналіз трафіку тощо;
* впровадження та використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);
* інші.

Перелік суттєвих загроз має бути максимально повним і деталізованим. Для кожної з загроз необхідно визначити її спрямованість, джерело, механізм реалізації та можливі наслідки.

**По-перше**, на порушення яких властивостей інформації або ІТС загроза спрямована:

- конфіденційності - несанкціоноване ознайомлення з інформацією;

- цілісності - несанкціонована модифікація (спотворення, фальсифікація, викривлення) інформації;

- доступності - порушення можливості використання ІТС або оброблюваної інформації (відмова в обслуговуванні користувача);

- спостереженості ІТС - відмова в ідентифікації, автентифікації та реєстрації небезпечних дій.

**По-друге**, джерела виникнення загрози (які суб’єкти ІТС або суб’єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу):

- персонал і користувачі;

- технічні засоби;

- моделі, алгоритми, програми;

- технологія функціонування;

- зовнішнє середовище.

**По-третє**, можливі способи здійснення (механізм реалізації) загроз:

* шляхом підключення до апаратури та ліній зв’язку;
* маскування під зареєстрованого користувача;
* подолання заходів захисту з метою використання інформації або нав’язування хибної інформації;
* застосування закладних пристроїв чи програм, впровадження шкідливих кодів і вірусів.

**По-четверте**, опис моделі загроз (у частині, що стосується переліку можливих способів реалізації загроз та їх класифікації) має бути викладений настільки детально, щоб дозволяти (на етапі аналізу ризиків, пов’язаних з реалізацією загроз) однозначне визначення як можливих наслідків у разі реалізації загрози, так і ймовірності її реалізації в певний спосіб.

**2.1 Перелік загроз з визначенням порушень властивостей**

**інформації та ІТС**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **№** | **Потенційні загрози для інформації в ІТС** | **Ризики для** | | | |
| **К** | **Ц** | **Д** | **С** |
| **1. Загрози об’єктивної природи** | | | | | |
| 1.1. | Стихійні явища (пожежа, аварії) |  | + | + | + |
| 1.2. | Збої та відмови системи електроживлення |  |  | + | + |
| 1.3. | Збої та відмови обчислювальної техніки |  |  | + | + |
| 1.4. | Збої, відмови та пошкодження носіїв інформації |  | + | + |  |
| 1.5. | Збої та відмови програмного забезпечення |  | + | + | + |
| **2. Загрози суб’єктивної природи** | | | | | |
| **2.1** | **Зовнішні загрози** |  |  |  |  |
| 2.1.1 | Несанкціоноване підключення до технічних засобів | + |  |  |  |
| 2.1.2 | Несанкціоноване підключення до каналів звязку | + |  |  |  |
| 2.1.3 | Читання даних, що виводяться на екран, роздруковуються, читання залишених без догляду документів | + |  |  |  |
| 2.1.4 | Несанкціоноване перехоплення інформації за рахунок витоку інформації за рахунок ПЕМВН | + |  |  |  |
| 2.1.5 | Несанкціонований перегляд інформації за рахунок візуально-оптичного каналу | + |  |  |  |
| **2.2** | **Порушення нормальних режимів роботи** |  |  |  |  |
| 2.2.1 | Зараження системи комп’ютерними вірусами |  | + | + | + |
| 2.2.2 | Втрата (розголошення) засобів розмежування доступу (паролів), магнітних носіїв інформації та резервних копій | + | + | + |  |
| 2.2.3 | Несанкціоноване внесення змін у технічні засоби, програмне забезпечення, компоненти інформаційного забезпечення тощо |  | + | + | + |
| 2.2.4 | Використання недозволеного програмного забезпечення або модифікація компонентів програмного та інформаційного забезпечення |  | + | + | + |
| 2.2.5 | Пошкодження носіїв інформації |  |  | + |  |
| 2.2.6 | Вхід у систему недопущених осіб (подолання систем захисту) | + | + | + |  |
| **2.3** | **Помилки персоналу** |  |  |  |  |
| 2.3.1 | Помилки користувачів (впровадження і використання програм, що не є необхідними для виконання службових обов’язків; запуск програм, здатних викликати критичні зміни в системі) | + | + | + |  |
| 2.4.2 | Помилки адміністраторів (неправильне конфігурування та адміністрування системи захисту, операційної системи; неправомірне відключення засобів захисту). | + | + | + |  |
| 2.3.3 | Порушення технології обробки, введення та виведення інформації, роботи з МНІ (резервними копіями, еталонами та дистрибутивами) | + | + | + |  |
| 2.3.4 | Недбале зберігання та облік документів, носіїв інформації, баз даних | + | + | + |  |
| 2.3.5 | Отримання сторонньою особою інформації у персоналу ІТС | + |  |  |  |

Зробимо розрахунок загроз з урахуванням 3-х рівнів ризиків і збитків:

- високий - якщо реалізація загрози надає великих збитків (3 бали);

- середній - якщо реалізація загрози надає помірних збитків (2 бали);

- низький - якщо реалізація загрози надає незначних збитків (1 бал).

**2.2 Модель загроз з визначенням рівня ризиків та збитків**

**1. Загрози конфіденційності інформації**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Механізм реалізації** | **Рівень** | | **Сума загроз** |
| **ризиків** | **збитків** |
| К.1 | Ненавмисне ознайомлення з ІзОД під час співбесід персоналу ІТС зі сторонніми особами | середній  2 | високий  3 | 5 |
| К.2 | Втрата носіїв ІзОД з причини безвідповідального ставлення до виконання обв’язків | низький  1 | високий  3 | 4 |
| К.3 | Перегляд ІзОД на екранах моніторів або робочих місцях користувачів ІТС сторонніми особами | середній  2 | високий  3 | 5 |
| К.4 | Копіювання ІзОД на зовнішні носії з метою несанкціонованого ознайомлення сторонніх осіб | високий  3 | високий  3 | 6 |
| К.5 | Роздрукування ІзОД з метою несанкціонованого ознайомлення сторонніх осіб | середній  2 | високий  3 | 5 |
| К.6 | Викрадення носіїв ІзОД з метою несанкціонованого ознайомлення сторонніх осіб | низький  1 | високий  3 | 4 |
| К.7 | Безпосередній доступ до ІзОД будь-яким способом сторонніх осіб | низький  1 | високий  3 | 4 |

**2. Загрози цілісності інформації**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Механізм реалізації** | **Рівень** | | **Сума загроз** |
| **ризиків** | **збитків** |
| Ц.1 | Помилки (ненавмисні) користувачів ІТС, які призвели до модифікації або спотворення інформації на жорсткому диску або зовнішніх носіях | середній  2 | середній  2 | 4 |
| Ц.2 | Несанкціонована (навмисне) модифікація або спотворення інформації персоналом ІТС на жорсткому диску або зовнішніх носіях | середній  2 | середній  2 | 4 |
| Ц.3 | Ненавмисне пошкодження носіїв інформації користувачами АС, яке призвело до модифікації або спотворення інформації | середній  2 | середній  2 | 4 |
| Ц.4 | Навмисне пошкодження носіїв інформації користувачами ІТС, яке призвело до модифікації або спотворення інформації | низький  1 | середній  2 | 3 |
| Ц.5 | Помилки (ненавмисні) адміністраторів ІТС при налагодженні засобів захисту та системного ПЗ, в наслідок яких стала можливою модифікація ІзОД | середній  2 | середній  2 | 4 |
| Ц.6 | Прояви помилок системного ПЗ, в наслідок яких стала можливою модифікація інформації або її спотворення користувачами | середній  2 | середній  2 | 4 |
| Ц.7 | Безпосередній доступ до інформації будь-яким способом сторонніми особами | низький  1 | середній  2 | 3 |

**3. Загрози доступності інформації**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Механізм реалізації** | **Рівень** | | **Сума загроз** |
| **ризиків** | **збитків** |
| Д.1 | Помилки (ненавмисні) користувачів ІТС, які призвели до знищення інформації або втрати доступу до неї | середній  2 | середній  2 | 4 |
| Д.2 | Помилки (ненавмисні) адміністраторів ІТС, які призвели до знищення інформації або втрати доступу | середній  2 | середній  2 | 4 |
| Д.3 | Некоректне налагодження засобів захисту АБ, яке призвело до втрати доступу до інформації або ІТС | середній  2 | середній  2 | 4 |
| Д.4 | Пошкодження парольних носіїв персоналом ІТС, що призвело до втрати доступу до інформації | середній  2 | середній  2 | 4 |
| Д.5 | Навмисне пошкодження парольних носіїв персоналом ІТС, яке призвело до втрати доступу до інформації | середній  2 | середній  2 | 4 |
| Д.6 | Прояви помилок системного ПЗ, яке призвело до втрати доступу до інформації або ІТС | середній  2 | середній  2 | 4 |
| Д.7 | Безпосередній доступ до ІТС будь-яким способом сторонніх осіб | низький  1 | середній  2 | 3 |

**4. Загрози спостереженості ІТС**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Механізм реалізації** | **Рівень** | | **Сума загроз** |
| **ризиків** | **збитків** |
| Н.1 | Помилки (ненавмисні) персоналу ІТС, які призвели до втрати спостереженості | низький  1 | середній  2 | 3 |
| Н.2 | Помилки (ненавмисні) адміністраторів ІТС, які призвели до втрати спостереженості | середній  2 | високий  3 | 5 |
| Н.3 | Некоректне налагодження засобів захисту адміністраторами ІТС, яке призвело до втрати спостереженості | низький  1 | високий  3 | 4 |
| Н.4 | Порушення спостережності користувачами ІТС внаслідок навмисного переповнення протоколів аудиту | середній  2 | середній  2 | 4 |
| Н.5 | Порушення спостереженості внаслідок пошкодження, у тому числі навмисного, поточних протоколів аудиту, архівів та носіїв з архівами протоколів аудиту | низький  1 | високий  3 | 4 |
| Н.6 | Прояви помилок системного ПЗ, яке призвело до втрати спостереженості | середній  2 | високий  3 | 5 |
| Н.7 | Безпосередній доступ до ІТС будь-яким способом сторонніх осіб | низький  1 | високий  3 | 4 |

**2.2.1 Модель загроз з розрахунком сумарного рівня ризиків та збитків.**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Види загроз** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **Сума загроз** |
| 1 | конфіденційності | 5 | 4 | 5 | 6 | 5 | 4 | 4 | 33 |
| 2 | спостереженості | 3 | 5 | 4 | 4 | 4 | 5 | 4 | 29 |
| 3 | доступності | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 27 |
| 4 | цілісності | 4 | 4 | 4 | 3 | 4 | 4 | 3 | 25 |

**2.3 Варіант моделі загроз для розподілених обчислювальних мереж**

(Матов О.Я., Василенко В.С. Модель загроз у розподілених мережах):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Вид загроз** | **Ймовір-ність** | **Що по-рушує** | **Рівень шкоди** | **Механізм реалізації** |
| **Моніторинг (розвідка) мережі** | | | | | |
| 1 | Розвідка, аналіз трафіка | висока | к, ц, д | відсутня | Перехоплення інформації, що пересилається, у незашифрованому вигляді в широкомовному середовищі передачі даних, відсутність виділеного каналу зв’язку між об’єктами РОМ |
| **Несанкціонований доступ до інформаційних ресурсів** | | | | | |
| 1 | Підміна (імітація) довіреного об’єкта або суб’єкта РОМ із підробкою мережних адрес тих об’єктів, що атакують | висока | к, ц, д | середній | Фальсифікація (підробка мережних адрес ІР-адреси, повторне відтворення повідомлень при відсутності вір туального каналу, недостатні ідентифікації та автентифікації при наявності віртуального каналу |
| 2 | Зміна маршрутизації | непри-пусти-мо висока | к, ц, д | низький | Зміна параметрів маршрутизації й змісту інформації, що передається, внаслідок відсутності контролю за маршрутом повідомлень чи відсутності фільтрації пакетів із невірною  адресою |
| 3 | Селекція потоку інформації та збереження її шляхом впровадження в розподілену обчислювальну систему хибних об’єктів (атаки типу «людина всередині») | висока | к, ц, д | високий | Використання недоліків алгоритмів віддаленого пошуку |
| 4 | Подолання систем адміністрування доступом до робочих станцій, локальних мереж і захищеного інформаційного об’єкта, заснованих на атрибутах робочих станцій чи засобів управління доступом і маршрутизації (маскування) відповідних мереж — (файрволів, проксі-серверів, маршрутизаторів тощо) | висока | к, ц, д | високий | Використання недоліків систем ідентифікації та автентифікації, заснованих на атрибутах користувача (ідентифікатори, паролі, біометричні дані та т.ін.). Недостатні ідентифікації та автентифікації об’єктів РОМ, зокрема, адреси відправника |
| **Специфічні загрози інформаційним об’єктам** | | | | | |
| 1 | Подолання криптографічної захищеності інформаційних об’єктів, що перехоплені | низька | к | високий | Використання витоків технічними каналами, вилучення із мережі специфічних вірусних атак шляхом впровадження програм-шпигунів (spyware) із розкриттям ключових наборів |
| 2 | Подолання криптографічної захищеності інформаційних об’єктів робочих станцій | низька | к | високий | Несанкціонований доступ до інформаційних об’єктів із використанням недоліків систем ідентифікації та автентифікації, заснованих на атрибутах користувача (ідентифікатори, паролі, біометричні дані та т.ін.) із розкриттям ключових наборів |
| 3 | Модифікація переданих даних, даних чи програмного коду, що зберігаються в елементах обчислювальних систем | висока | ц, д | високий | Модифікація чи підміна інформаційних об’єктів (програмних кодів) чи їхніх частин шляхом впровадження руйнуючих програмних засобів чи зміни логіки роботи програмного файлу із використанням спеціальних типів вірусних атак, спроможних здійснити те чи інше порушення цілісності |
| 4 | Блокування сервісу чи перевантаження запитами системи управління доступом (відмова в обслуговуванні) | висока | д | високий | Використання атак типу «спрямований шторм» (Syn Flood), передачі на об’єкт, що атакується, некоректних, спеціально підібраних запитів |
| Використання анонімних (чи із модифікованими адресами) запитів на обслуговування типу електронної пошти (spam) чи вірусних атак спеціального типу |

**Контрольні питання**

Що необхідно визначити після проведення обстеження всіх середовищ ІТС?

Яким може бути походження загроз?

Які є найбільш відомі випадкові загрози?

Яким чином визначається сутність відмови?

Яким чином визначається сутність збою?

Яким чином визначається сутність помилки?

Яким чином визначається сутність побічного впливу?

Якими можуть бути передумови появи загроз?

Чим можуть бути спричинені об'єктивні передумови появи загроз?

Яка діяльність відноситься до суб'єктивних передумов появи загроз?

За якими критеріями класифікуються всі можливі канали витоку інформації?

На скільки класів поділяються всі можливі канали витоку інформації?

Як проявляються канали витоку інформації 1-го класу?

Як проявляються канали витоку інформації 2-го класу?

Як проявляються канали витоку інформації 3-го класу?

Як проявляються канали витоку інформації 4-го класу?

Як проявляються канали витоку інформації 5-го класу?

Як проявляються канали витоку інформації 6-го класу?

Що розробляє СЗІ на підставі акту обстеження та моделі порушника?

Що має містити модель загроз для інформації?

На які види поділяються загрози, що мають суб'єктивну природу?

Що таке випадкові загрози суб’єктивної природи?

Що таке навмисні загрози суб’єктивної природи?

Які складові кожної з загроз необхідно визначити в Моделі загроз?

Яку властивість ІзОД можна порушити в результаті її копіювання на зовнішні носії?

Яку властивість ІзОД можна порушити в результаті її спотворення?

Яку властивість ІзОД можна порушити в результаті її знищення?

Яку властивість ІТС можна порушити в результаті її перевантаження запитами?

Яку властивість ІТС можна порушити в результаті переповнення протоколів її аудиту?