**Заняття 4. Лекція 5. Модель порушника безпеки інформації.**

**Вступ.**

**Питання 1. Класифікація потенційних порушників безпеки інформації.**

**Питання 2. Формування моделі порушника.**

**Питання 3. Висновки.**

**Контрольні питання.**

**Вступ.**

На підставі Акту обстеження та визначення загроз для ІТС СЗІ розробляють «Модель порушника безпеки інформації в ІТС», яка затверджується керівником організації-власника (розпорядника) ІТС, та вноситься, за необхідності, до відповідних розділів Плану захисту.

Модель порушника - це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії тощо. Як порушник розглядається особа, яка може одержати несанкціонований доступ (далі - НСД) до роботи з включеними до складу ІТС засобами.

Модель порушника повинна визначати:

* можливі цілі порушника та їх градація за ступенями небезпечності для ІТС та інформації, що потребує захисту;
* категорії персоналу, користувачів ІТС та сторонніх осіб, із числа яких може бути порушник;
* припущення про кваліфікацію порушника;
* припущення про характер його дій.

Метою порушника можуть бути:

* отримання необхідної інформації у потрібному обсязі та асортименті;
* мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
* нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

**Питання 1.**

Порушники спочатку поділяються на дві основні групи: зовнішні та внутрішні.

Зовнішніх порушників можна розділити на:

- добре озброєну та технічно оснащену групу, що діє зовні швидко і напролом;

- поодиноких порушників, що не мають допуску на об'єкт і намагаються діяти потайки й обережно, так як вони усвідомлюють, що сили реагування мають перед ним переваги.

Сторонні особи, що можуть бути порушниками:

- клієнти (представники організацій, громадяни);

- відвідувачі (запрошені з якого-небудь приводу);

- представники організацій, взаємодіючих з питань забезпечення систем життєдіяльності організації (енерго-, водо-, теплопостачання тощо);

- представники конкуруючих організацій (іноземних служб) або особи, що діють за їх завданням;

- особи, які випадково або навмисно порушили пропускний режим (без мети порушити безпеку);

- будь-які особи за межами контрольованої зони.

Потенціальних внутрішніх порушників можна розділити на:

- допоміжний персонал об'єкту, що допущений на об'єкт, але не допущений до життєво важливого центру ІТС;

- основний персонал, що допущений до життєво важливого центру (найбільш небезпечний тип порушників);

- співробітників служби безпеки, які часто формально не допущені до життєво важливого центру ІТС, але реально мають достатньо широкі можливості для збору необхідної інформації і скоєння акції.

Серед внутрішніх порушників можна виділити такі категорії персоналу:

- користувачі (оператори) системи;

- персонал, що обслуговує технічні засоби (інженери, техніки);

- співробітники відділів розробки та супроводження програмного забезпечення (прикладні та системні програмісти);

- технічний персонал, що обслуговує будівлю (прибиральниці, електрики, сантехніки та інші співробітники, що мають доступ до будівлі та приміщення, де розташовані компоненти ІТС);

- співробітники служби безпеки;

- керівники різних рівнів та посадової ієрархії.

Крім професійного шпигунства, можна виділити три основних мотиви порушень: безвідповідальність, самоствердження та корисливий інтерес.

При порушеннях, викликаних безвідповідальністю, користувач цілеспрямовано або випадково виробляє руйнуючі дії, які не пов'язані проте зі злим умислом. У більшості випадків це наслідок некомпетентності або недбалості. Деякі користувачі вважають одержання доступу до системних наборів даних значним успіхом, затіваючи свого роду гру заради самоствердження або у власних очах, або в очах колег.

Порушення безпеки ІТС може бути викликано корисливим інтересом користувача ІТС. У цьому випадку він буде цілеспрямовано намагатися подолати систему захисту для несанкціонованого доступу до інформації в ІТС.

Усіх порушників можна класифікувати за такими ознаками:

за рівнем знань про ІТС;

- за рівнем можливостей;

- за часом дії;

- за місцем дії.

За рівнем знань про ІТС (в залежності від кваліфікації та професійної майстерності):

- володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС;

- володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування;

- володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС;

- знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості.

За рівнем можливостей (в залежності від методів і засобів, що використовуються):

- застосовує чисто агентурні методи отримання відомостей;

- застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);

- використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні носії інформації, які можуть бути тайком пронесені крізь пости охорони;

- застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, перехоплення з каналів передачі даних, впровадження спеціальних програмних закладок).

За часом дії (в залежності від активності або пасивності системи):

- у процесі функціонування (під час роботи компонентів системи);

- у період неактивності системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування та ремонтів і т.д.);

- як у процесі функціонування, так і в період неактивності системи.

За місцем дії (в залежності від території доступу до засобів системи):

- без доступу на контрольовану територію організації;

- з контрольованої території без доступу до будівель та споруджень;

- усередині приміщень, але без доступу до технічних засобів;

- з робочих місць кінцевих користувачів (операторів);

- з доступом у зону даних (баз даних, архівів тощо);

- з доступом у зону управління засобами забезпечення безпеки.

Враховуються також такі обмеження та припущення про характер дій можливих порушників:

- робота з підбору та розстановки кадрів, а також заходи контролю за персоналом ускладнюють можливість створення коаліцій порушників, тобто злочинного угрупування (змови) і цілеспрямованих дій з подолання системи захисту двох і більше порушників;

- порушник, плануючи спробу НСД, приховує свої несанкціоновані дії від інших співробітників;

- НСД може бути наслідком помилок користувачів, адміністраторів, а також хиб прийнятої технології обробки інформації тощо.

Припускається, що в своєму рівні порушник - це фахівець вищої кваліфікації, який має повну інформацію про ІТС і засоби захисту. Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

**Питання 2.**

Під час формування моделі порушника обов'язково повинно бути визначено:

- ймовірність реалізації загрози,

- своєчасність виявлення,

- відомості про порушення.

Слід зауважити, що всі злочини, зокрема і комп’ютерні, здійснюються людиною. Користувачі ІТС, з одного боку, є її складовою частиною, а з іншого - основною причиною і рухаючою силою порушень і злочинів. Отже, питання безпеки захищених ІТС фактично є питанням людських відносин та людської поведінки.

**Модель порушників можна відобразити системою таблиць**, наприклад:

Для побудови моделі використовуються усі можливі категорії, ознаки та характеристики порушників для більш точного їх аналізу, причому рівень загрози кожної з них вказується в дужках і оцінюється за 4-бальною шкалою.

Таблиця 1. Категорії порушників, визначених у моделі

|  |  |  |
| --- | --- | --- |
| Позначення | Визначення категорії | Рівень загрози |
| Внутрішні по відношенню до ІТС | | |
| ПВ1 | Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС | 1 |
| ПВ2 | Персонал, який обслуговує технічні засоби ІТС (інженери, техніки) | 2 |
| ПВ3 | Користувачі (оператори) ІТС | 2 |
| ПВ4 | Адміністратори ІТC, співробітники служби захисту інформації | 3 |
| ПВ5 | Співробітники служби безпеки установи та керівники різних рівнів | 4 |
|  | Зовнішні по відношенню до ІТС |  |
| ПЗ1 | Відвідувачі (запрошені з будь-якого приводу) | 1 |
| ПЗ2 | Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше) | 2 |
| ПЗ3 | Хакери | 3 |
| ПЗ4 | Агенти конкурентів або закордонних спецслужб «під прикриттям» | 4 |

Таблиця 2. Специфікація моделі порушника за мотивами здійснення порушень

|  |  |  |
| --- | --- | --- |
| Позначення | Мотив порушення | Рівень загрози |
| М1 | Безвідповідальність | 1 |
| М2 | Самоствердження | 2 |
| М3 | Корисливий інтерес | 3 |
| М4 | Професійний обов’язок (ПЗ4) | 4 |

Таблиця 3. Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

|  |  |  |
| --- | --- | --- |
| Позначення | Основні кваліфікаційні ознаки порушника | Рівень загрози |
| К1 | Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС | 1 |
| К2 | Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування | 2 |
| К3 | Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС | 3 |
| К4 | Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості | 4 |

Таблиця 4. Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

|  |  |  |
| --- | --- | --- |
| Позначення | Характеристика можливостей порушника | Рівень загрози |
| З1 | Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях | 1 |
| З2 | Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС | 2 |
| З3 | Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону | 3 |
| З4 | Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації | 4 |

Таблиця 5. Специфікація моделі порушника за часом дії

|  |  |  |
| --- | --- | --- |
| Позначення | Характеристика можливостей порушника | Рівень загрози |
| Ч1 | Під час повної бездіяльності ІТС з метою відновлення та ремонту | 1 |
| Ч2 | Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації | 2 |
| Ч3 | Під час функціонування ІТС (або компонентів системи) | 3 |
| Ч4 | Як у процесі функціонування ІТС, так і під час призупинки компонентів системи | 4 |

Таблиця 6. Специфікація моделі порушника за місцем дії

|  |  |  |
| --- | --- | --- |
| Позначення | Характеристика місця дії порушника | Рівень загрози |
| Д1 | Усередині приміщень, але без доступу до технічних засобів ІТС | 1 |
| Д2 | З робочих місць користувачів (операторів) ІТС | 2 |
| Д3 | З доступом у зону зберігання баз даних, архівів тощо | 3 |
| Д4 | З доступом у зону керування засобами забезпечення безпеки ІТС | 4 |

Виведемо два варіанти сумарного рівня загроз

для окремих категорій можливих порушників:

1) внутрішній порушник «ПВ» - варіант мінімальних загроз з причини безвідповідального ставлення до виконання своїх посадових обов’язків;

2) зовнішній порушник «ПЗ4» (агент конкурентів або закордонних спецслужб «під прикриттям») - варіант максимальних загроз з причини цілеспрямованих несанкціонованих дій з метою модифікації або викрадення інформації.))

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Категорія поруш-ника | Мотив пору-шення | Рівень обізнано-сті щодо ІТС | Можливості щодо подолання системи захисту | Можли-вості за часом дії | Можли-вості за місцем дії | Сума загроз (посада) |
| ПВ1 | М1 | К1 | З1 | Ч4 | Д1 | **9**  **(прибир-ця)** |
| 1 | 1 | 1 | 1 | 4 | 1 |
| ПЗ4 | М4 | К4 | З4 | Ч4 | Д1 | **21**  **(електрик)** |
| 4 | 4 | 4 | 4 | 4 | 1 |
| ПВ1 | М1 | К1 | З1 | Ч1 | Д1 | 8 |
| 1 | 1 | 1 | 1 | 3 | 1 |
| ПЗ4 | М4 | К4 | З4 | Ч1 | Д1 | 20 |
| 4 | 4 | 4 | 4 | 3 | 1 |
| ПВ2 | М1 | К2 | З1 | Ч4 | Д3 | 12 |
| 2 | 1 | 2 | 1 | 4 | 2 |
| ПЗ4 | М4 | К4 | З4 | Ч4 | Д3 | 22 |
| 4 | 4 | 4 | 4 | 4 | 2 |
| ПВ3 | М1 | К2 | З1 | Ч3 | Д2 | 11 |
| 2 | 1 | 2 | 1 | 3 | 2 |
| ПЗ4 | М4 | К4 | З4 | Ч3 | Д2 | 21 |
| 4 | 4 | 4 | 4 | 3 | 2 |
| ПВ4 | М1 | К4 | З1 | Ч4 | Д4 | **17**  **(кор-чі)** |
| 3 | 1 | 4 | 1 | 4 | 4 |
| ПЗ4 | М4 | К4 | З4 | Ч4 | Д4 | **24**  **(Технік)** |
| 4 | 4 | 4 | 4 | 4 | 4 |
| ПВ5 | М1 | К1 | З1 | Ч4 | Д3 | **14**  **(адмін-я)** |
| 4 | 1 | 1 | 1 | 4 | 3 |
| ПЗ4 | М4 | К4 | З4 | Ч4 | Д3 | **23**  **(безпека)** |
| 4 | 4 | 4 | 4 | 4 | 3 |

Після зведення усіх даних 1-го варіанту в одну таблицю отримаємо таку табличну

**«Модель внутрішнього порушника політики безпеки інформації»**:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Категорія порушника «ПВ» | Мотив пору-шення | Рівень обізна-ності щодо ІТС | Можливості щодо подолання системи захисту | Можли-вості за часом дії | Можли-вості за місцем дії | Сума загр |
| Служба безпеки | М1 | К1 | З1 | Ч4 | Д3 | 14 |
| Адмініст-ратор ІТС | М1 | К4 | З1 | Ч4 | Д4 | 17 |
| Користувач | М1 | К2 | З1 | Ч3 | Д2 | 11 |
| Технік ІТС | М1 | К2 | З1 | Ч4 | Д3 | 12 |
| Електрик | М1 | К1 | З1 | Ч1 | Д1 | 8 |
| Прибираль-ниця | М1 | К1 | З1 | Ч4 | Д1 | 9 |

**Питання 3.**

З останньої таблиці видно, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становить адміністратор ІТС. Тому організація роботи цієї особи повинна бути найбільш контрольованою, оскільки вона є основним потенційним порушником безпеки інформації.

Те, що основною загрозою для безпеки інформації в ІТС є персонал ІТС, підтверджують і дані, опубліковані у 2010 році американським інститутом комп′ютерної безпеки (Сан-Франциско, штат Каліфорнія), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин:

- несанкціонований доступ - 2%;

- ураження вірусами - 3%;

- технічні відмови апаратури мережі - 20%;

- цілеспрямовані дії персоналу - 20%;

- помилки персоналу (недостатній рівень кваліфікації) - 55%.

Таким чином, основною потенційною загрозою для інформації в ІТС слід вважати цілеспрямовані або випадкові деструктивні дії персоналу, оскільки вони становлять 75 % усіх випадків.

**Контрольні питання**

Що таке Модель порушника безпеки інформації?

Яка особа розглядається як порушник безпеки інформації?

Які припущення визначає Модель порушника безпеки інформації?

На які дві основні групи спочатку поділяються порушники?

За якими ознаками класифікуються порушники безпеки інформації?

В залежності від чого класифікуються порушники за рівнем знань про ІТС?

В залежності від чого класифікуються порушники за рівнем можливостей?

В залежності від чого класифікуються порушники за місцем дії?

В залежності від чого класифікуються порушники за часом дії?

Яка робота ускладнює можливість створення коаліцій порушників?

Що обов'язково повинно бути визначено під час формування моделі порушника?

Які порушники становлять найбільшу загрозу для безпеки інформації в ІТС?

Хто є основним потенційним порушником безпеки інформації в ІТС?