**Класифікація загроз безпеки**

Під загрозою безпеки розуміють потенційні дії або події, які можуть прямо чи опосередковано принести втрати – привести до розладу, спотворення чи несанкціонованого використання ресурсів мережі, включаючи інформацію, що зберігається, передається або обробляється, а також програмні і апаратні засоби.

Не існує єдиної загальноприйнятої класифікації загроз, хоча існує багато її варіантів. Приведемо перелік тем подібних класифікацій:

- по цілі реалізації;

- по принципу дії на систему;

- по характеру впливу на систему;

- по причині появи помилки захисту;

- по способу дії атаки на об’єкт;

- по об’єкту атаки;

- по використовуваних засобах атаки;

- по стану об’єкту атаки.

Загрози прийнято ділити на випадкові (або ненавмисні) і навмисні. Джерелом перших можуть бути помилки в ормальнее у забезпеченні, виходи з ладу апаратних засобів, неправильні дії користувачів або адміністрації локальної обчислювальної мережі і, так далі. Навмисні загрози, на відміну від випадкових, прагнуть нанести шкоду користувачам (абонентам) локальної обчислювальної мережі і, в свою чергу, діляться на активні і пасивні. Пасивні загрози, як правило, спрямовані на несанкціоноване використання інформаційних ресурсів локальної обчислювальної мережі, не впливаючи при цьому на її функціонування. Нормальне загрозою є, наприклад, спроба отримання інформації, що циркулює в каналах передачі даної локальної обчислювальної мережі, шляхом підслуховування. Активні загрози прагнуть порушити нормальне функціонування локальної обчислювальної мережі шляхом цілеспрямованого впливу на її апаратні, програмні і інформаційні ресурси. До активних загроз відносяться, наприклад, порушення або радіоелектронне заглушення ліній зв’язку локальної обчислювальної мережі, вивід з ладу ЕОМ або її операційної системи, спотворення відомостей в користувацьких базах даних або системної інформації локальної обчислювальної мережі і т.д. Джерелами активних загроз можуть бути безпосередні дії зловмисників, програмні віруси і, так далі.

**Основні види загроз безпеки інформації**

До основних загроз безпеки інформації відносяться:

- розкриття конфіденційної інформації:

- компрометація інформації;

- несанкціоноване використання ресурсів локальної обчислювальної мережі;

- помилкове використання її ресурсів;

- несанкціонований обмін інформацією;

- відмова від інформації;

- відмова в обслуговуванні.

Засобами реалізації загрози розкриття конфіденційної інформації може бути несанкціонований доступ до баз даних, прослуховування каналів локальної обчислювальної мережі і, так далі. В кожному випадку, отримання інформації, що є власністю деякої особи (чи групи), наносить її власникам суттєву шкоду.

Компрометація інформації, як правило, здійснюється шляхом внесення несанкціонованих змін в бази даних, в результаті чого її користувач змушений або відмовитись від неї або витратити додаткові зусилля для виявлення змін і відновлення істинних відомостей. У випадку використання скомпрометованої інформації користувач може прийняти невірні рішення з усіма наслідками, що звідси випливають.

Несанкціоноване використання ресурсів локальної обчислювальної мережі, з однієї сторони, є засобом розкриття або компрометації інформації, а з іншої – має самостійне значення, оскільки, навіть не торкаючись користувацької або системної інформації, може нанести певні збитки абонентам або адміністрації локальної обчислювальної мережі. Обсяги збитків можуть змінюватися в широких межах – від скорочення поступлення фінансових ресурсів до повного виходу мережі з ладу.

Помилково санкціоноване використання ресурсів локальної обчислювальної мережі теж може призвести до знищення, розкриття або компрометації вказаних ресурсів. Така загроза найчастіше всього є наслідком помилок програмного забезпечення локальної обчислювальної мережі.

Несанкціонований обмін інформацією між абонентами локальної обчислювальної мережі може призвести до отримання одним із них відомостей, доступ до яких йому заборонений, що по своїх наслідках рівно сильно розкриттю інформації.

Відмова від інформації полягає в невизнанні адресатом чи відправником цієї інформації, фактів її отримання або відправки. Це, зокрема, може послужити аргументованим приводом до відмови однією з сторін від раніше підтриманої угоди (фінансової, торгової, дипломатичної тощо) «технічним шляхом», формально не відмовившись від неї, тим самим може нанести іншій стороні значні збитки.

Відмова в обслуговуванні – це дуже суттєва і достатньо розповсюджена загроза, джерелом якої є сама локальна комп’ютерна мережа. Подібна відмова особливо небезпечна в ситуаціях, коли затримка з наданням ресурсів мережі абоненту може привести до тяжких для нього наслідків. Наприклад, відсутність у абонента даних, необхідних для прийняття рішень може бути причиною його нераціональних або неоптимальних дій.