***Аналіз загроз інформаційної безпеки,***

***які можуть бути реалізовані на об’єкті***

*Загроза* – будь-які обставини або події, що можуть бути причиною порушення безпеки об’єкта та нанесення збитків.

На цьому етапі визначається перелік загроз інформаційної безпеки, проводиться аналіз можливих ризиків з боку цих загроз.

В залежності від виду об’єкту та специфіки його функціонування, по різному можуть проявляти себе і загрози, характерні для цього об’єкта.

Визначення та систематизація переліку загроз, які виникають у відповідності до кожної окремої сукупності об’єктів захисту, здійснюється виходячи із усіх можливих джерел виникнення загроз.

Перелік можливих загроз інформаційним ресурсам та засобам їх обробки визначається виходячи із можливих шляхів утворення каналів витоку інформації та можливих випадкових та навмисних впливів на інформаційні системи.

Витік інформації з нашого об’єкта захисту може відбуватись за рахунок:

Вікна можуть служити каналом витоку акустичної та візуальної інформації, а також можливе фізичне проникнення в приміщення об’єкта захисту. На вікна необхідно поставити грати, двійні вікна, зовнішнє – візерункове, внутрішнє – товщиною не менше 1 см, або генератори шумів.

Також одним із каналів витоку інформації є двері. Через двері можливо одержати акустичну та візуальну інформацію, а також можливе фізичне проникнення в приміщення, отже потрібно поставити двійні броньовані двері, оббити їх шкірою, для захисту від витоку акустичної та візуальної інформації та для запобігання фізичного проникнення зловмисника. Двері повинні бути з надійними замками.

Стіни також можуть бути каналом витоку інформації. Оскільки в стінах є комунікації, провідники та розетки. Також через стіну можна отримати акустичну інформацію. Важливим є матеріал з якого виготовлені стіни. Потрібно щоб вони були цегляні і чим грубші - тим краще. В розетки необхідно вставити пластмасові заглушки, вони будуть не пропускати акустичну інформацію, яку можна отримати через провідники, які ведуть до розетки.

Через стелю може реалізуватись канали електричного наведення. Захист стін залежить від того, на якому поверсі знаходить наше приміщення.

Система вентиляції є також одним із каналів витоку інформації. Через систему вентиляції можна реалізувати такі загрози: проникнення, прослуховування, тобто витік акустичної інформації, а також досить просто порушити роботу персоналу при подачі в систему вентиляції різних газів чи інших речовин. Отже потрібно поставити грати на певні елементи системи вентиляції, а саме на отвори, які виходять на ззовні приміщення. Також необхідно поставити вентилятори, які би створювали невеликий шум, і водночас виконували свою функцію. Також можна поставити повітряні фільтри.

Через каналізаційний колодязь можна отримати інформацію, яка стосується виробництва підприємства. По відходам можна визначити речовини якими користуються або виробляють на підприємстві. Особливу небезпеку витік такої інформації небезпечний для хімічних лабораторій чи хімічних підприємств.

Завдяки люку водопостачання на об’єкті захисту можна реалізувати такі загрози: порушення доступності інформації, спровокувати аварію чи перекрити воду.

Трансформаторна підстанція є також небезпечним каналом витоку інформації. Загрози: відключення енергії, тому підстанцію необхідно закривати на ключ, в підстанції є багато провідників через які можна отримати інформацію, а також вони можуть служити антенами для зловмисника.

Проводи заземлення: інформаційний канал наведення, електромагнітне наведення. Необхідно ставити фільтри.

Завдяки машинам, розміщених на території контрольованої зони, можна прослуховувати, реалізувати електромагнітне наведення, вести відео нагляд за територією об’єкта захисту.

Також, необхідно контролювати працівників КПП. Необхідно виплачувати їм достатньо високу зарплату, для запобігання підкупу працівників. Те саме стосується усіх працівників об’єкта захисту. Забезпечити нагляд працівниками КПП за особами які мають на меті пройти на об’єкт захисту. Необхідно забезпечити перепустки для працівників підприємства, та тимчасові перепустки для відвідувачів.

Через огорожу можливе фізичне проникнення, тому необхідно забезпечити нагляд працівників КПП за огорожею. А також необхідно щоб огорожа була не менша ніж 2-2,5м висотою. І при необхідності ставити огорожу під струм.

Так, як шосе знаходиться за межами контрольованої зони, то з цього боку можна реалізувати такі загрози, як фізичне знищення захисту чи самого об’єкта, проникнення через огорожу. Також шосе є потенційною загрозою для об’єкта захисту

Отже, можна зробити такий висновок: несанкціоноване ознайомлення з таємною інформацією з метою її подальшого використання є можливим шляхом перехоплення зловмисниками такої інформації. Для цього зловмисник може використовувати широкий арсенал портативних засобів, які дозволяють здійснювати перехоплення різних форм інформації. В залежності від виду об’єкту та специфіки його функціонування, по різному можуть проявляти себе і загрози, характерні для цього об’єкта. Визначення та систематизація переліку загроз, які виникають у відповідності до кожної окремої сукупності об’єктів захисту, здійснюється виходячи із усіх можливих джерел виникнення загроз. При попередньому уточненні можливих загроз, головну увагу потрібно концентрувати на інформаційних сигналах та полях, середовищі їх поширення та засобах їх обробки. Тому перелік можливих загроз інформаційним ресурсам та засобам їх обробки визначається виходячи із можливих шляхів утворення каналів витоку інформації та можливих випадкових та навмисних впливів на інформаційні системи.