Реферат

На тему:

«Методи і засоби захисту інформації»

Методи захисту інформації

Установка перешкоди – метод фізичного перегородило шляху зловмиснику до інформації, що захищається, у тому числі спроб з використанням технічних засобів знімання інформації і дії на неї.

Управління доступом – метод захисту інформації за рахунок регулювання використовування всіх інформаційних ресурсів, у тому числі автоматизованої інформаційної системи підприємства. Управління доступом включає наступні функції захисту:

• ідентифікацію користувачів, персоналу і ресурсів інформаційної системи (привласнення кожному об'єкту персонального ідентифікатора);

• аутентифікацію (встановлення автентичності) об'єкту або суб'єкта по пред'явленому їм ідентифікатору;

• перевірку повноважень (перевірка відповідності дня тижня, часу доби, запрошуваних ресурсів і процедур встановленому регламенту);

• дозвіл і створення умов роботи в межах встановленого регламенту;

• реєстрацію (протоколювання) звернень до ресурсів, що захищаються;

• реагування (сигналізація, відключення, затримка робіт, відмова в запиті) при спробах несанкціонованих дій.

Маскування – метод захисту інформації з використанням інженерних, технічних засобів, а також шляхом криптографічного закриття інформації.

Маскувальники аналогово-цифровые статичні.

Скремблери – Маскувальники аналогово-цифрові динамічні.

Вокодери – пристрої, що передають мову в цифровому вигляді і зашифрованому.

Методи захисту інформації на практиці реалізуються із застосуванням засобів захисту.

Засоби захисту інформації

Засоби захисту інформації можна розділити на:

1. Засоби, призначені для захисту інформації. Ці засоби не призначені для безпосередньої обробки, зберігання, накопичення і передачі інформації, що захищається, але що знаходяться в одному приміщенні з ними.

Діляться на:

пасивні – фізичні (інженерні) засоби, технічні засоби виявлення, ПС, СЬКУД, ВН, прилади контролю радіоефіру, ліній зв'язку і т.п.;

активні – джерела безперебійного живлення, шумогенератори, скремблери, пристрої відключення лінії зв'язку, програмно-апаратні засоби маскування інформації і ін.

2. Засоби, призначені для безпосередньої обробки, зберігання, накопичення і передачі інформації, що захищається, виготовлені в захищеному виконанні. НІЇЕВМ РБ розробляє і випускає захищені ношені, возяться і стаціонарні ПЕВМ.

3. Засоби, призначені для контролю ефективності захисту інформації.

Пасивні засоби захисту акустичного і віброакустичного каналів просочування мовної інформації.

Для запобігання просочування мовної інформації по акустичному і віброакустичному каналам здійснюються заходи щодо виявлення каналів витоку. В більшості випадків для несанкціонованого знімання інформації з приміщення супротивник застосовує відповідні задуму заставні пристрої.

Всю процедуру пошуку ЗУ можна умовно розбити на декілька етапів:

• фізичний пошук і візуальний огляд;

• виявлення радіозаставних пристроїв як електронних засобів;

• перевірка наявності каналів просочування інформації.

Фізичний пошук і візуальний огляд

Огляд здійснюється шляхом обстеження всіх предметів в зоні контролю, розміри яких достатньо великі для того, щоб можна було розмістити в них технічні засоби негласного знімання інформації (настільні прилади, рами картин, телефони, квіткові горщики, книги, живлені від сіті пристрою: комп'ютери, ксерокси, радіоприймачі і т.д.).

Фізичний пошук і візуальний огляд об'єктів проводять із застосуванням спеціальних засобів відеоспостереження і металлодетекторів.

Виявлення радіозаставних пристроїв (РЗУ)

Незнайдених при візуальному огляді здійснюють по їх демаскуючих ознаках із застосуванням спеціальних засобів виявлення. РЗУ, як правило, містять в своїй конструкції електронні схеми і, при своїй роботі випромінюють радіосигнал.

Основними ознаками випромінювання радіозакладок є:

* відносно високий рівень випромінювання, обумовлений необхідністю передачі сигналу за межі контрольованого приміщення.
* безперервна або безперервна протягом деякого часу робота (переривистий режим роботи вдень і практично, повне мовчання вночі; випромінювання виникає одночасно з підняттям трубки і зникає, коли трубка встановлена).
* поява нового джерела в звичайно вільному частотному діапазоні.
* використовування у ряді радіозакладок направлених антен приводить до сильної локалізації випромінювання, тобто істотної нерівномірності його рівня в межах контрольованого об'єкту.
* особливості поляризації випромінювання радіозакладок. При зміні просторового положення або орієнтації приймальної антени спостерігається зміна рівня всіх джерел. Проте однотипні видалені джерела одного діапазону поводяться приблизно однаково, тоді як сигнал закладки змінюється відмінно від інших. Ефект поляризації виявляється при використовуванні аналізаторів спектру.
* зміна («розмивання») спектру випромінювань радіомікрофонів при виникненні яких-небудь шумів в контрольованому приміщенні. Він виявляється тільки в тому випадку, якщо РЗУ працює без кодування передаваної інформації.

До основних пристроїв, вживаних для виявлення РЗУ відносяться:

– індикатори поля;

– спеціальні радіоприймачі;

– програмно-апаратні комплекси радіоконтроля;

– нелінійні радіолокатори.

Індикатори поля – прилади визначаючі наявність ЗУ по їх радіовипромінюванню. Індикатори, або детектори поля є найпростішими засобами виявлення факту використовування радіозакладок. Це приймачі з низькою чутливістю, тому вони знаходять випромінювання радіозаставних пристроїв на гранично малих відстанях (10–40 см), ніж і забезпечується селекція «нелегальних випромінювань» на фоні могутніх «дозволених сигналів». Важлива гідність детекторів – здатність знаходити передаючі пристрої незалежно від вживаної в них модуляції. Основний принцип пошуку полягає у виявленні абсолютного максимуму рівня випромінювання в приміщенні.

Іноді детектори використовують і в так званому сторожовому режимі. В цьому випадку після повної перевірки приміщення на відсутність ЗУ фіксується рівень поля в деякій точці простору (звичайно це стіл керівника або місце ведення переговорів), і прилад переводиться в черговий режим. У разі включення закладки (приблизно на видаленні до двох метрів від детектора), індикатор видає сигнал про підвищення рівня електромагнітного поля. Проте необхідно враховувати той факт, що якщо використовуватиметься радіозакладка з дуже низьким рівнем випромінювання, то детектор швидше за все не зафіксує її активізацію.

Спеціальні радіоприймальні пристрої

Радіоприймальні пристрої, як пристрої виявлення радіозакладок, повинні задовольняти трьом основним умовам:

• мати нагоду настройки на частоту роботи пристроїв, таємно передаючих перехоплену інформацію, тобто мати нагоду контролювати великий набір частот або одночасно у всьому діапазоні або перебудовуючись від значення до значення за гранично малий проміжок часу – панорамні приймачі;

• володіти функціями виділення потрібного сигналу по характерних ознаках сигналів і перешкод, що на фоні заважають (вибірковість по спектру частот);

• володіти здібністю до демодуляції різних видів сигналів (позбавлятися від сигналу несучої частоти, а корисний сигнал перетворювати в низькочастотний сигнал і демодулювати за допомогою детектора, відповідного типу використаної модуляції).

Програмно-апаратні комплекси радіоконтроля

Для розширення можливостей спеціальних приймачів їх функціонально суміщають з персональними комп'ютерами, що істотно підвищує надійність і оперативність пошуку ЗУ, робить процедуру виявлення більш зручної (технологічної).

На комп'ютер при цьому покладається рішення наступних задач:

• зберігання апріорної інформації про радіоелектронні засоби, що працюють в контрольованій області простору і вибраних діапазонах частот;

• отримання програмними методами тимчасових і частотних характеристик сигналів, що приймаються;

• тестування сигналів, що приймаються, по сукупності ознак на приналежність до випромінювання ЗУ.

Програмно-апаратні комплекси радіоконтроля забезпечують:

• виявлення випромінювань РЗУ;

• пеленгація РЗУ в реальному масштабі часу;

• визначення дальності до джерел випромінювання;

• аналого-цифрову обробку сигналів з метою визначення їх приналежності до випромінювання РЗУ;

• контроль силових, телефонних, радіотрансляційних і інших сітей;

• роботу в багатоканальному режимі, що дозволяє контролювати декілька об'єктів одночасно;

• постановку прицільних перешкод на частотах випромінювання РЗУ і ін.

Програмно-апаратні комплекси радіоконтроля складаються з наступних елементів:

• широкодіапазонного перебудовуваного по частоті приймача (сканера);

• блоку розпізнавання РЗУ, що здійснює ідентифікацію випромінювань радіомікрофонів на основі порівняння прийнятих сигналів, що детектують, з природним акустичним фоном приміщення (пасивний спосіб) або тестовим акустичним сигналом (активний спосіб);

• блоку акустичної локації, що дозволяє по запізнюванню перевипроміненного зондуючого звукового імпульсу визначати відстань до активних радіомікрофонів;

• електронно-обчислювальної машини (процесора), що здійснює як обробку отриманих даних, так і управління приймачем.

За принципом побудови всі відомі прилади даного класу діляться на дві основні групи:

• спеціально розроблені комплекси, конструктивно виконані у вигляді єдиного пристрою;

• комплекси, сформовані на базі серійного сканера, персонального комп'ютера (звичайно notebook) і спеціального програмного забезпечення.

Нелінійні радіолокатори

Застосовуються для пошуку упроваджених РЗУ, що не використовують радіоканал для передачі інформації, а також РЗУ, що знаходяться в пасивному (невипромінюючому) стані.

Нелінійні радіолокатори – прилади, випромінюючі електромагнітну хвилю з частотою f, а приймаючі перевипромінені сигнали на частотах f. Якщо такі сигнали будуть знайдені, то в зоні дії локатора є напівпровідникові елементи, і їх необхідно перевірити на можливу приналежність до ЗУ. Нелінійний радіолокатор знаходить тільки радіоелектронну апаратуру і, на відміну від класичного лінійного радіолокатора, не «бачить» віддзеркалень від навколишніх предметів, тобто володіє високою вибірковістю. Джерелами перешкод для його роботи можуть служити контакти із слабим притиском, для яких характерний наявність проміжного окисного шару.

Активні технічні засоби захисту акустичного і віброаккустичного каналу

Для активного захисту мовної інформації від незнайдених заставних пристроїв і знімання по інших каналах використовується апаратура активного захисту:

* Технічні засоби просторового зашумлення;
* Пристрої віброакустичного захисту;
* Технічні засоби ультразвукового захисту.

##### Технічні засоби просторового і лінійного зашумлення

За принципом дії всі технічні засоби просторового і лінійного зашумлення можна розділити на три великі групи:

засоби створення акустичних маскуючих перешкод:

* генератори шуму в акустичному діапазоні;
* пристрої віброакустичного захисту;
* технічні засоби ультразвукового захисту приміщень;

засоби створення електромагнітних маскуючих перешкод:

* технічні засоби просторового зашумлення;
* технічні засоби лінійного зашумлення, які у свою чергу діляться на засоби створення маскуючих перешкод в комунікаційних сітях і засоби створення маскуючих перешкод в сітях електроживлення;
* багатофункціональні засоби захисту.

Генератори шуму в акустичному діапазоні

Основний принцип радіоелектронної протидії – створення перешкод для приймального пристрою з інтенсивністю, достатньою для порушення його роботи.

Якщо наперед невідома його робоча частота, то необхідно створити перешкоду по всьому можливому або доступному діапазону спектру. Достатньо універсальною перешкодою для зв'язних радіоліній вважається шумовий сигнал. У зв'язку з цим апаратура радіопротидії повинна включати в свій склад генератор шуму достатньої потужності (на необхідний діапазон) і антенну систему. Практично при відношенні верхньої і нижньої частоти діапазону більш 2‑х використовують декілька шумових генераторів і комбінована багатодіапазонна антена.

Генератори шуму в мовному діапазоні використовуються для захисту від несанкціонованого знімання акустичної інформації шляхом маскування безпосередньо корисного звукового сигналу. Маскування проводиться «білим шумом» з коректованою спектральною характеристикою.

Зразковий вид структурної схеми джерела акустичного шуму приведений на рис. 1. Конструктивно апаратура включає блок формування і посилення шумового сигналу і декілька акустичних випромінювачів.

Излучатель акустического шума № 1

Генератор шума

Излучатель акустического шума №.Х

Рис. 1. Структурна схема джерела акустичного шуму

В деяких випадках наявність декількох випромінювачів необов'язково. Тоді використовуються компактні генератори з вбудованою акустичною системою, акустичний генератор білого шуму.

Головний недолік застосування джерел шумів в акустичному діапазоні – це неможливість комфортного проведення переговорів. Практика показує, що в приміщенні де «реве» генератор шуму неможливо знаходитися більше 10…15 мін. Крім того, співбесідники автоматично починають намагатися перекричати засіб захисту, знижуючи ефективність його застосування. Тому подібні системи застосовуються для додаткового захисту дверних отворів, міжрамного простору вікон, систем вентиляції і т.д.

Пристрої віброакустичного захисту

Пристрої віброакустичного захисту використовуються для захисту приміщень, призначених для проведення конфіденційних заходів, від знімання інформації через шибки, стіни, системи вентиляції, труби опалювання, двері і т.д. Дана апаратура дозволяє запобігти можливому прослуховуванню за допомогою дротяних мікрофонів, звукозаписної апаратури, радіомікрофонів і електронних стетоскопів, лазерного знімання акустичної інформації з вікон і т.д. Протидія прослуховуванню забезпечується внесенням віброакустичних шумових коливань в елементи конструкції будівлі.

Конструктивно апаратура включає блок формування і посилення шумового сигналу і декількох акустичних і віброаккустичних випромінювачів (рис. 2). Генератор формує «білий шум» в діапазоні звукових частот. Передача акустичних коливань на захищаючі конструкції проводиться за допомогою п'єзоелектричних (на основі пєзокераміки) або електромагнітних вібраторів з елементами кріплення. Конструкція і частотний діапазон випромінювачів повинна забезпечувати ефективну передачу вібрації. Вібропреобразователі порушують шумові віброколивання в захищаючих конструкціях, забезпечуючи при цьому мінімальний рівень перешкоджаючого акустичного сигналу в приміщенні, практично не впливаючий на комфортність проведення переговорів.

Передбачена в більшості виробів можливість підключення акустичних випромінювачів, дозволяє «зашумляти вентиляційні канали» і дверні тамбури. Як правило, є можливість плавного регулювання рівня шумового акустичного сигналу. При цьому треба орієнтуватися на те, що відновити перехоплене повідомлення практично неможливо, якщо рівень перешкоди більш ніж в 10 разів перевищує рівень сигналу у всьому частотному діапазоні (відношення сигнал / перешкода менш – 20 дБ).

Технічні засоби ультразвукового захисту приміщень

Відмітною особливістю технічних засобів УК захисту є дія на мікрофонний пристрій і його підсилювач достатньо могутнім ультразвуковим сигналом (групою сигналів), що викликає блокування підсилювача або виникнення значних нелінійних спотворень, що приводять, кінець кінцем, до порушення працездатності мікрофонного пристрою (його придушенню).

Оскільки дія здійснюється по каналу сприйняття акустичного сигналу, то абсолютно не важливі його подальші трансформації і способи передачі. Акустичний сигнал пригнічується саме на етапі його сприйняття чутливим елементом. Все це робить комплекс достатньо універсальним в порівнянні з іншими засобами активного захисту. При цьому не відбувається істотного зниження ергономічних характеристик приміщення.

Багатофункціональні засоби захисту

При практичній організації захисту приміщення від просочування інформації по технічних каналах необхідне комплексне використовування різних пристроїв безпеки: акустичних, віброаккустичних, мережних генераторів шуму і джерел електромагнітного маскуючого випромінювання. При цьому можна піти наступними трьома шляхами:

* підбором різних пристроїв захисту інформації і їх автономним використовуванням;
* об'єднанням різних пристроїв захисту інформації в єдиний комплекс шляхом застосування універсального блоку управління і індикації;
* використовуванням готових комплектів.

Література

1. Барсуков В.С. Безпека: технології, засоби, послуги / В.С. Борсуків. – М., 2001 – 496 с.

2. Ярочкин В.И. Інформаційна безпека. Підручник для студентів вузів / 3‑е изд. – М.: Академічний проект: Трікста, 2005. – 544 з.

3. Барсуков В.С. Сучасні технології безпеки / В.С. Борсуків, В.В. Водолазській. – М.: Нолідж, 2000. – 496 з., мул.

4. Зегжда Д.П. Основи безпеки інформаційних систем / Д.П. Зегжда, А.М. Івашко. – М.: Гаряча лінія – телеком, 2000. – 452 с., мул.

5. Комп'ютерна злочинність і інформаційна безпека / А.П. Леонов [і др.]; під общ. Ред. А.П. Леонова. – Мінськ: АРІЛ, 2000. – 552 с.