УДК 004.056

Грабар Марія Володимирівна,

студентка VI курсу Харківського національного університету радіоелектроніки,

Олейніков Анатолій Миколайович,

к.т.н., професор, кафедра інформаційних радіотехнологій і технічного захисту інформації Харківського національного університету радіоелектроніки

ЗАБЕЗПЕЧЕННЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ОБ'ЄКТІВ

Анотація. У роботі розглянуто основні аспекти забезпечення технічного захисту інформаційних систем та об'єктів від несанкціонованого доступу, витоку інформації та інших загроз інформаційній безпеці. Проаналізовано основні технічні канали витоку інформації, сучасні методи й засоби її захисту, а також організаційні та технічні заходи, спрямовані на підвищення рівня захищеності інформаційних ресурсів. Особливу увагу приділено виявленню потенційних загроз, оцінюванню ризиків та впровадженню комплексних систем технічного захисту інформації. Визначено значення застосування сучасних технологій для забезпечення конфіденційності, цілісності та доступності інформації.

Ключові слова: технічний захист інформації, інформаційна безпека, інформаційні системи, канали витоку інформації, засоби захисту.

За метою впливу розрізняють три основні типи загроз безпеці

інформаційних систем:

- загрози порушення конфіденційності інформації;
- загрози порушення цілісності інформації;
- загрози порушення працездатності системи (відмови в обслуговуванні).

Загрози порушення конфіденційності направлені на розголошення конфіденційної чи секретної інформації. При реалізації цих загроз інформація стає відомою особам, які не повинні мати до неї доступ.

Загрози порушення цілісності інформації, що зберігається в комп'ютерній системі чи передається по каналу зв'язку, направлені на її зміну чи спотворення, що приводить до порушення її якості чи повного знищення. Цілісність інформації може бути порушена спеціально зловмисноком, а також в результаті впливу зовнішнього середовища, що оточує систему.

Загрози порушення працездатності (відмова в обслуговуванні) направлені на створення таких ситуацій, коли певні навмисні дії або знижують працездатність ІС, або блокують доступ до її ресурсів. [1]

Утворенню технічних каналів витоку інформації сприяють певні обставини і причини технічного характеру. До ним можна віднести недосконаліть елементної бази і схемних рішень (конструкторських, технологічних), експлуатаційний знос елементів пристроїв(зміна характеристик, аварійний вихід із строю), а також зловмисні дії (зміна характеристик, створення аварійних ситуацій, блокування засобів захисту).

Основними джерелами утворення технічних каналів витоку інформації є:

- акустичні перетворювачі (індуктивні, ємкісні, п'єзоелектричні, оптичні);
- випромінювачі електромагнітних коливань (низькочастотні, високочастотні, оптичні);

- паразитні зв'язки і наведення (обернений зв’язок, по ланцюгам живлення, по ланцюгам заземлення) [2]

Для надійної охорони інформаційних систем та об’єктів треба проаналізувати всі можливі технічні канали витоку інформації:

1. Акустичний канал витоку інформації: можливий витік інформації через прослуховування стін або дверей. Для захисту приміщення від прослуховування через стіни встановлюються спеціальні матеріали на стіни, які зменшують передачу звуку і електромагнітних хвиль (в даному випадку, стіна покрита звукопоглинаючим матеріалом). Додатково можливими варіантами витоку інформації є її отримання за допомогою закладних пристроїв, лазерних систем акустичної розвідки (ЛСАР), а також через комунікаційні конструкції будівлі, зокрема трубопроводи систем опалення та водопостачання.

Для зниження ризику витоку інформації акустичним каналом передбачається комплекс організаційних та технічних заходів. До таких заходів належить проведення регулярного радіомоніторингу з метою виявлення можливих закладних пристроїв та інших засобів технічної розвідки. Віконні конструкції доцільно встановлювати у вигляді двокамерних склопакетів із підвищеними звукоізоляційними характеристиками.

2. Радіоелектронний канал витоку інформації: для оцінювання можливості витоку інформації радіоелектронним каналом враховуються побічні електромагнітні випромінювання технічних засобів, зокрема монітора ПЕОМ та можливості реєстрації їх за межами контрольованої зони.

З метою зниження можливості витоку інформації через побічні електромагнітні випромінювання доцільним є застосування комплексу технічних заходів, спрямованих на зменшення рівня випромінювання та обмеження її поширення за межі контрольованої зони. До таких заходів

можуть належати екранування технічних засобів або приміщення, фільтрація відповідних комунікацій, а також контроль рівних побічних електромагнітних випромінювань за межами контрольованої зони.

3. Електричний канал витоку інформації: він пов’язаний із можливістю поширення небезпечних інформаційних сигналів через електричні мережі, заземлювальні ланцюги та інші провідні комунікації, що виходять за межі виділеного приміщення та контрольованої зони.

Для зниження можливості витоку інформації через електромережу доцільно передбачити екранування загального трифазного кабелю, а також взяти теплостанцію під контроль охорони.

Окремо необхідно врахувати систему заземлення об’єкта. Для зниження можливості витоку інформації через систему заземлення рекомендується застосовувати багатоточкову схему заземлення технічних засобів та здійснювати регулярний моніторинг стану заземлення.

4. Візуально-оптичний канал витоку інформації: він пов’язаний із можливістю несанкціонованого отримання інформації шляхом безпосереднього візуального спостереження за інформаційною системою або об’єктом із застосуванням оптичних та оптико-електронних засобів технічної розвідки. Основним елементом приміщення, через який може реалізовуватися такий канал, є віконні конструкції.

Для зниження можливості витоку інформації через візуально-оптичний канал необхідно обмежити можливості спостереження за приміщеннями через віконні конструкції. З цією метою вікна можуть обладнуватися спеціальними жалюзі, які обмежують можливість візуального спостереження та ускладнюють застосування оптичних та оптико-електронних засобів технічної розвідки (біноклі, телескопи, фото- та відеокамери, телескопічні/довгофокусні об’єктиви тощо). Додатково доцільно не допускати розміщення біля вікон документів, екранів та інших носіїв інформації, доступних для візуального спостереження.

5. Матеріально-речовий канал витоку інформації: він пов’язаний із можливістю несанкціонованого отримання конфіденційної інформації внаслідок потрапляння носія інформації до осіб, які не мають відповідного права доступу до них. Для досліджуваного об’єкта (інформаційної системи) такий канал може реалізовуватись шляхом винесення за межі приміщення або КЗ матеріальних носіїв, на яких міститься конфіденційна інформація. До потенційних матеріальних носіїв інформації належать чернетки та інші документи, що містять інформацію обмеженого доступу, макети пристроїв, відходи діловодства, а також електронні носії, зокрема CD-флешки, флеш-накопичувачі та жорстокі диски.

Особливу увагу потрібно приділяти контролю персоналу, оскільки внутрішній порушник, маючи законний доступ до приміщення та матеріальних носіїв інформації, потенційно може здійснити їх несанкціоноване переміщення за межі КЗ. Для попередження такого витоку службі безпеки необхідно регулярно проводити аудит серед персоналу та контролювати переміщення матеріальних носіїв інформації. Додатковим методом виявлення можливого несанкціонованого отримання інформації персоналом може бути навмисне дезінформування.

Для зниження витоку всі матеріальні носії, що містять конфіденційну інформацію, повинні зберігатись у спеціально обладнаних приміщеннях або знищуватись із застосуванням відповідних засобів. Чернетки документів та відходи діловодства, які можуть містити інформацію обмеженого доступу, не повинні залишатись у вільному доступі. Електронні носії після завершення їх використання також підлягають контрольованому зберіганню або знищенню.

Список використаних джерел

1. Основні загрози безпеці інформаційних систем. StudFiles. URL: https://studfile.net/preview/5118185/page:42/.
2. 1.Класифікація каналів витоку інформації. StudFiles. URL: https://studfile.net/preview/9276384/.