Національна безпека

УДК 004.931

Ярутіч Альона Олександрівна
магістрант
Навчально-наукового інституту інформаційної безпеки
Національної академії Служби безпеки України

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

Анотація. *Розглянуто поняття захисту інформації та можливі технічні канали витоку інформації, а також заходи здійснення захисту інформації від витоку вказаними каналами.*

Ключові слова: *інформація, захист інформації, канали витоку інформації, технічні канали витоку інформації, заходи захисту інформації, виявлення закладних пристроїв, екранування, заземлення, звукоізолювання, канали перехоплення інформації.*

Актуальність роботи. Інформація, яка є важливою для особи, суспільства та держави і втрата якої може спричинити шкоду особі, суспільству або національним інтересам держави в економічній, політичній, військової або інших сферах, повинна захищатися від несанкціонованого ознайомлення спотворення, знищення та блокування, тобто бути об'єктом захисту.

Обов'язковість захисту певної інформації встановлена відповідними законами України [5].

Захисту від витоку технічними каналами на об'єкті інформаційної діяльності (далі – ОІД) підлягає інформація, що становить державну таємницю. Захист іншої інформації з обмеженим доступом (далі – ІзОД) від витоку технічними каналами на ОІД здійснюється за рішенням

розпорядника цієї інформації.

Створення комплексу ТЗІ передбачає проведення організаційних, інженерних і технічних заходів на ОІД, а саме:

- озвучення ІзОД (при проведенні нарад, під час показів зі звуковим супроводженням кіно- і відеофільмів тощо);
- здійснення обробки ІзОД технічними засобами (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання ІзОД тощо);
- обіг іншої ІзОД при проектуванні, будівництві, експлуатації об'єктів, виробництві технічних засобів тощо [3].

Мета даної статті: сформувати загальне уявлення про захист інформації, та конкретно про захист інформації від витоку технічними каналами.

1. Визначення понять «інформація», «захист інформації», «канал витоку інформації» та «технічний канал витоку інформації»

Відповідно до ст.1 Закону України «Про інформацію», інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [2].

Під витоком інформації розуміється неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання.

Витік інформації відбувається відповідним каналом витоку. Оскільки засоби розвідки противника, як правило, технічні, то і канали витоку також називають технічними [5].

Процесом утворення каналу витоку інформації називається утворення паразитної (небажаної) послідовності (ланцюжка) носіїв

інформації, один (або декілька) з яких може бути правопорушником або його спеціальною апаратурою.

А отже, канал витоку інформації – паразитний ланцюжок носіїв інформації, один (або декілька) з яких може бути правопорушником або його спеціальною апаратурою [1].

Технічний канал витоку інформації (ТКВІ) - сукупність джерела небезпечного сигналу, середовища поширення небезпечного сигналу та засобу технічної розвідки.

Тобто, технічним каналом витоку інформації є фізичний шлях небезпечного сигналу (носія інформації) від джерела небезпечного сигналу до противника [5].

Під технічним каналом витоку інформації (ТКВІ), також, розуміють сукупність об'єкта розвідки, технічного засобу розвідки (ТЗР), за допомогою якого видобувається інформація про цей об'єкт, і фізичного середовища, в якому поширюється інформаційний сигнал. По суті, під ТКВІ розуміють спосіб отримання за допомогою ТЗР розвідувальної інформації про об'єкт. Причому під розвідувальною інформацією звичайно розуміються відомості чи сукупність даних про об'єкти розвідки незалежно від форми їх подання.

Сигнали є матеріальними носіями інформації. По своїй фізичній природі сигнали можуть бути електричними, електромагнітними, акустичними, і т.д. Тобто сигналами, як правило, є електромагнітні, механічні та інші види коливань (хвиль), причому інформація міститься в їх параметрах, які змінюються.

Залежно від природи, сигнали розповсюджуються в певних фізичних середовищах. У загальному випадку, середовищем поширення можуть бути газові (повітряні), рідинні (водні) і тверді середовища. Наприклад повітряний простір, конструкції будівель, з'єднувальні лінії і струмопровідні елементи, грунт (земля) і т. д. [6].

2. Класифікація технічних каналів витоку інформації

Для встановлення вимог та організації захисту інформації від витоку технічними каналами здійснена їх класифікація за певними ознаками.

За видом інформаційної діяльності на ОІД відокремлюються такі типи ТКВІ:

1) технічні канали витоку мовної інформації,
2) технічні канали витоку інформації, що обробляється в ОТЗС,
3) технічні канали витоку візуальної інформації,
4) матеріально-речовинні канали витоку інформації.

Класифікацію ТКВІ за принципом (фізичним ефектом, процесом) формування небезпечного сигналу, середовищем поширення небезпечного сигналу та способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника доцільно розглянути у межах визначених вище типів ТКВІ.

Технічні канали витоку мовної інформації за цими ознаками поділяються на такі:

1. Акустичні канали.
2. Акустовібраційні (віброакустичні) канали.
3. Акустооптоелектронні (лазерні акустичні) канали.
4. Акустоелектричні канали.
5. Відеоакустичні канали.
6. Канали ВЧ нав'язування (для зняття мовної інформації).
7. Канали витоку мовної інформації на основі закладних пристроїв.

Технічні канали витоку інформації, що обробляється в ОТЗС, поділяються на такі:

1. Канали побічних електромагнітних випромінювань.
2. Канали побічних електромагнітних наведень.
3. Канали "паразитної" модуляції сигналів ВЧ генераторів.

4. Канали "паразитної" ВЧ генерації підсилювачів.

5. Канали перехоплення (зняття) інформації з волоконно-оптичних ліній передачі даних.

6. Канали перехоплення (зняття) інформації з каналів зв'язку.

7. Канали ВЧ нав'язування (длязняття інформації, що обробляється в ОТЗС).

8. Канали витоку інформації, що обробляється в ОТЗС, на основі закладних пристроїв.

Технічні канали витоку візуальної інформації поділяються на такі:

1. Візуальні канали.

2. Візуально оптичні канали.

3. Канали витоку візуальної інформації на основі закладних пристроїв.

Матеріально-речовинні канали витоку інформації:

1. Добування інформації з магнітних та інших носіїв інформації засобів ЕОТ, що вийшли з ладу.

2. Добування інформації з чернеток документів, з відходів виробництва, видавницької діяльності, діловодства тощо.

3. Хімічні канали.

За носієм інформації та принципом формування небезпечного сигналу відокремлюються такі ТКВІ:

електромагнітні канали витоку інформації;

електричні канали витоку інформації;

параметричні канали витоку інформації.

За місцем перехоплення інформації засобами технічної розвідки противника відокремлюються такі типи ТКВІ:

1) канали перехоплення (зняття) інформації за межами КЗ,

2) канали перехоплення (зняття) інформації за межами КЗ з активним впливом на параметри технічного каналу витоку інформації

(наприклад, канал ВЧ нав'язування),

3) канали зняття інформації засобами технічної розвідки, встановленими на ОІД (наприклад, технічні канали витоку інформації закладними пристроями).

Розглянута класифікація технічних каналів витоку інформації дозволяє систематизувати уявлення про них та встановити вимоги і заходи щодо захисту інформації від витоку відповідними ТКВІ [5].

3. Методи й засоби захисту інформації від витоку технічними каналами

Захист інформації від витоку технічними каналами забезпечують проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також виявленням портативних закладних пристроїв [4, 6].

Організаційні заходи - це спрямовані на захист інформації заходи, проведення яких не потребує спеціально розроблених технічних засобів.

До основних організаційних заходів відносять:

- залучення до робіт для захисту інформації організацій, що мають ліцензії відповідних органів на діяльність в області технічного захисту інформації (ТЗІ);
- категорування й атестацію об'єктів ТЗПІ та приміщень, виділених для проведення секретних заходів (виділених приміщень) щодо відповідності вимогам забезпечення захисту інформації під час проведення робіт з відомостями відповідного ступеня секретності;
- використання на об'єкті сертифікованих ТЗПІ та ДТЗС;
- встановлення КЗ навколо об'єкта;
- залучення до робіт із монтування апаратури, будування чи реконструкції об'єктів ТЗПІ організацій з відповідними ліцензіями;
- організацію контролю та обмеження доступу на об'єкти ТЗПІ та у виділені приміщення;

- введення територіальних, частотних, енергетичних, просторових і часових обмежень у режимах використання технічних засобів, що підлягають захисту;

- відключення технічних засобів, що мають елементи властивостей електроакустичних перетворювачів, від ліній зв'язку на період проведення секретних заходів.

Технічні заходи - це спрямовані на захист інформації заходи, проведення яких передбачає використання спеціальних технічних засобів, а також реалізацію технічних рішень.

Технічні заходи слугують для закриття каналів витоку інформації за рахунок ослаблення рівня інформаційних сигналів або зменшення відношення сигнал/завада у місцях можливого розміщення ТЗР або їх датчиків до рівнів, що унеможливлюють виділення інформаційних сигналів засобами розвідки. Під час проведення таких заходів використовують активні та пасивні методи.

До технічних заходів із використанням пасивних методів відносять:

1. контроль і обмеження доступу на об'єкти ТЗПІ та у виділені приміщення;

2. локалізація випромінювання (екранування ТЗПІ та з'єднувальних ліній, заземлення ТЗПІ та екранів їх з'єднувальних ліній, звукоізолювання виділених приміщень)

3. розв'язування інформаційних сигналів (установлення спеціальних захисних засобів типу Граніт, Рікас у ДТЗС із мікрофонним ефектом і таких, що мають вихід за межі КЗ; установлення спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалення, водозабезпечення і каналізації, що виходять за межі КЗ; установлення автономних або стабілізованих пристроїв електроживлення ТЗПІ (наприклад, мотор-генераторів); установлення в мережах електроживлення ТЗПІ, а в лініях освітлювальної та розеткової мережі

виділених приміщень- завадоподавляючих фільтрів типу ФП, ФСП, ФС-2).

До технічних заходів із використанням активних методів належать:

1. просторове зашумлення (просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних завад відповідними засобами; створення акустичних і вібраційних завад із використанням генераторів акустичного шуму - шумотронів; подавлення працюючих у режимі запису диктофонів за допомогою подавляючих пристроїв).

2. лінійне зашумлення (мереж електроживлення та кіл заземлення; сторонніх дротів та з'єднувальних ліній ДТЗС, що виходять за межі КЗ).

3. знешкодження підключених до лінії закладних пристроїв за допомогою спеціальних генераторів імпульсів (випалювачів «жучків»).

Виявити закладні пристрої можна завдяки спеціальним обстеженням (візуальний огляд без залучення технічних засобів) і спеціальним перевіркам (із використанням технічних засобів) об'єктів ТЗПІ та виділених приміщень.

Для виявлення закладних пристроїв використовують:

1) пасивні методи (установлення засобів і систем виявлення лазерного випромінювання (підсвітлення скла на вікнах); установлення стаціонарних детекторів диктофонів; розшук закладних пристроїв за допомогою індикаторів поля, інтерсепторів, частотомірів, сканувальних приймачів та програмно-апаратних комплексів контролю; організація радіоконтролю (постійно або на час проведення конфіденційних заходів) побічних електромагнітних випромінювань ТЗПІ);

2) активні методи (спеціальна перевірка виділених приміщень із використанням нелінійних локаторів; спеціальна перевірка виділених приміщень, ТЗПІ та ДТЗІ з використанням рентгенівських комплексів).

Висновок. Отже, ми бачимо, що різного роду інформація для різних

об'єктів інформаційної діяльності може мати велику цінність та бути предметом витоку технічними каналами. До них відносяться: канали витоку мовної, візуальної інформації та інші, що дає змогу зловмисникам знаходити найбільш зручні варіанти. Тому й доцільно на кожному ОІД здійснювати захист цінної інформації та цим самим унеможливити її витік.

Література

1. Громико І. О. Загальна парадигма захисту інформації: визначення термінів від носіїв до каналів витоку інформації / І. О. Громико // Системи обробки інформації. — Х.: ХУПС, 2006. — Вип. 9 (58). — С. 3-9.
2. Закон України «Про інформацію», м. Київ, 2 жовтня 1992 року N2657-XII.
3. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
4. Рекомендации по оценке защищенности конфиденциальной информации от ее утечки за сет ПЭМИ / Куренков Е.В., Лысов А.В., Остапенко А.Н. - Защита информации. – 1998. – № 4. – С. 48-50.
5. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. - К.: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с.
6. Хорев А.А. «Защита информации от утечки по техническим каналам. Часть1. Технические каналы утечки информации». – Москва, 1997.