УДК 621.39

Мурза С.П.

ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ АКУСТИЧНИМИ КАНАЛАМИ

Вінницький національний технічний університет

Анотація

В даній роботі розглядаються важливість захисту мовної інформації від витоку, проаналізовано методи та засоби захисту інформації від витоку акустичними каналами, визначено основні проблемні питання (загальносистемного та специфічного характеру), пов'язані зі створенням комплексів технічного захисту інформації (КТЗІ) на об'єктах інформаційної діяльності.

Ключові слова: інформація, захист інформації, мовна інформація, комплекс технічного захисту інформації, об'єкт інформаційної діяльності.

Abstract

The work considers the importance of protecting the linguistic information from leakage, analyzes the methods and means of protecting information from leakage by acoustic channels, identifies the main problem issues (system-wide and specific) related to the creation of information security information protection complexes (ITCs) at information objects .

Keywords: information, information protection, language information, complex of technical protection of information, object of information activity.

Вступ

На сьогоднішній день, не дивлячись активне використання автоматизованих та комп'ютеризованих систем обробки інформації, людська мова залишається одним із найважливіших шляхів інформаційної взаємодії. Більш того, при децентралізації економічної і політичної систем і відповідному збільшенні частки оперативної інформації, що безпосередньо зв'язує самостійних в ухваленні рішень людей, значущість мовного обміну зростає. Одночасно зростає потреба в забезпеченні конфіденційності мовного обміну, тому необхідно визначити які ж існують методи та засоби захисту інформації [1].

Основна частина

Захист інформації від витоку технічними каналами забезпечують за допомогою проектно-архітектурних рішень, проведення організаційних та технічних заходів, а також виявлення портативних закладних пристроїв [2].

Технічні заходи – це заходи спрямовані на захист інформації, які характеризуються використанням спеціальних технічних засобів, а також реалізацією технічних рішень [3].

Технічні заходи використовують для усунення каналів витоку інформації за рахунок зниження рівня інформаційних сигналів або зменшення відношення сигнал/перешкода у місцях можливого розміщення технічного засобу розвідки (ТЗР) або їх датчиків до рівнів, перешкоджають виділенню інформаційних сигналів засобами розвідки. Для проведення таких заходів використовують пасивні та активні методи [4].

До технічних заходів із використанням пасивних методів відносять такі [5]:

1. контроль та обмеження доступу на об'єкти технічних засобів приймання, обробки, зберігання та передання інформації (ТЗПІ) та у відведених приміщеннях (встановлення на об'єктах ТЗПІ та у відведених приміщеннях технічних засобів та систем обмеження і контролю доступу);
2. локалізація випромінювання:

– звукоізолювання відведених приміщень;

– заземлення ТЗПІ та екранів їх з'єднувальних ліній;
– екранування ТЗПІ та з'єднувальних ліній.

3. розв'язання інформаційних сигналів:

– встановлення спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалення, водозабезпечення і каналізації, що виходять за межі контрольної зони (КЗ);
– встановлення спеціальних захисних засобів типу Граніт, Рікас у допоміжних технічних засобах і системах (ДТЗС) із мікрофонним ефектом і таких, які мають вихід за межі КЗ;
– встановлення автономних або ж стабілізованих пристроїв електроживлення ТЗПІ (наприклад, мотор-генераторів);
– встановлення 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 такі [6]:

1. просторове зашумлення:

– створення акустичних і вібраційних завад за допомогою генераторів акустичного шуму – шумотронів;
– просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних завад відповідними засобами (за умови виявлення та з'ясування частоти випромінювання закладного пристрою або ПЕМВ ТЗПІ);
– 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;

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

Висновки

Безперервне вдосконалення як технологій, так і засобів негласного знімання мовної інформації, що підтверджується зростаючими витратами на розробку і виробництво відповідної апаратури, потребує, згідно з логікою організації протидії, певної уваги до методів та засобів захисту. Щоб гарантувати високу ступінь захисту мовної інформації, необхідно постійно вирішувати складні науково-технічні завдання щодо розробки та вдосконалення засобів і способів її захисту.

Таким чином, безпека мовної інформації досягається комплексним застосуванням апаратних, програмних і криптографічних методів, і засобів захисту, а також організаційних заходів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи‖ для студентів напрямів підготовки 6.030601 – „Менеджмент‖ та 6.170103 – ―Управління інформаційною безпекою‖ / Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с
2. ТЗІ. [Електронний ресурс]. – Режим доступу: https://tzi.ua/ua/zahist_movno_nformac.html. – Захист мовної інформації.
3. Методи та засоби захисту інформації. [Електронний ресурс]. – Режим доступу: http://www.bestreferat.ru/referat218628.html. – Оцінка витоку акустичної інформації для контрольваного приміщення.
4. Абрамов Ю.В., Калиниченко М.В., Каргашин В.Л. Досвід практичних робіт по віброакустичному захисту виділених приміщень від просочування мовної інформації // Науково-практична конференція "Ключові проблеми банківської безпеки" Третього московського міжнародного форуму "Технологія безпеки - 98". 1998.
5. Маслов О.Н. Защита акустической информации: резервы системного подхода / О.Н. Маслов, В.Ф. Шашенков // Методы и технологии защиты информации в технических каналах связи. – 2013. – №1. – С. 30-35.
6. Хорев А.А. Методы защиты речевой информации и оценки их эффективности / А.А. Хорев, Ю.К. Макаров // Защита информации. Конфидент. – 2001. – №4. – С. 22-33.

Мурза Сергій Павлович – студент групи КІН – 18мі, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: murza_serhiy@ukr.net

Науковий керівник: **Людмила Миколаївна Ткачук** – канд. економічних наук, доцент кафедри МБІС, Вінницький національний технічний університет, м. Вінниця.

Murza Serhii - student group UB-14b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsya, e-mail: murza_serhiy@ukr.net

Scientific supervisor: **Liudmyla Tkachuk** – cand. economic sciences, Assistant Professor of Building MBIS, Vinnitsa National Technical University, Vinnitsa,