Сарокіна Владислава Володимирівна
Національний університет «Одеська юридична академія»
студентка 4-го курсу факультету кібербезпеки
та інформаційних технологій

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ЕЛЕКТРОМАГНІТНИМ КАНАЛОМ

Актуальність даної теми полягає у тому, що на сьогоднішній день захист інформації від перехоплення за рахунок побічних електромагнітних випромінювань і наведень є однією з найважливіших задач в загальному комплексі заходів щодо забезпечення інформаційної безпеки об'єкта технічного захисту інформації. Це пов'язано з тим, що в даний час широко застосовуються різні технічні засоби обробки інформації. Сама по собі інформація, що обробляється за допомогою технічних засобів являє собою найбільшу цінність, так як вона є найбільш простою в обробці, а перехоплення електромагнітних випромінювань дає можливість отримання доступу до оброблюваної інформації без прямого доступу до пристрою користувача. Об'єктами технічного захисту інформації є установи системи державного управління, військові і військово-промислові об'єкти, науково-дослідні установи і т.д.

Сам по собі захист інформації від витоку по електромагнітним каналах являє собою конкретний комплекс розроблених заходів, які виключають зовсім або ж знижують ступінь ймовірного неконтрольованого виходу інформації (як правило, конфіденційної) за межі зони, яка знаходиться під контролем, за рахунок електромагнітних полів побічного характеру [1].

Конструкторсько-технологічні заходи щодо локалізації можливості утворення умов виникнення каналів витоку інформації за рахунок побічних електромагнітних випромінювань і наведень у технічних засобах обробки і передачі інформації зводяться до раціональним конструкторсько-технологічним рішенням, до числа яких відносяться: спеціальні матеріали, що забезпечують зниження рівня паразитних електромагніт-

них випромінювань за межами виділених приміщень (поглинання і екранування); системи активної маскування, що створюють в разведопасних напрямках перешкоди, які знижують ймовірність перехоплення випромінювань; технічні засоби обробки інформації в захищеному виконанні. Для виключення можливості використання технічною розвідкою струмопровідних комунікацій, що виходять за межі зони, що охороняється, застосовуються засоби блокування, екранування і лінійного зашумлення.

Загалом, можна виділити наступні електромагнітні канали витоку інформації: мікрофонний ефект елементів електронних схем; електромагнітне випромінювання низької або високої частоти; виникнення паразитної генерації підсилювачів різного призначення; ланцюги харчування і кола заземлення електронних схем; взаємний вплив проводів і ліній зв'язку; високочастотне нав'язування волоконно-оптичні системи [3].

На сьогоднішній день найбільш відомими методами захисту інформації від витоку по електромагнітним шляхам є активний та пасивний метод захисту.

Суть активного методу захисту інформації полягає в застосуванні спеціальних широкосмугових передавачів перешкод. Його перевагою є те, що скасовується не тільки загроза витоку інформації по каналах електромагнітного випромінювання, але й деякі інші види загроз. Як правило, унеможливлюється прослуховування шляхом застосування закладних пристроїв, також стає неможливою використання випромінювання всіх інших пристроїв, що знаходяться у даному приміщені, з цілю проведення розвідки. Його недоліками можна назвати: наявність приховуваного випромінювання свідчить про те, що в даному приміщенні є інформація, що захищається, а це, саме по собі, привертає до відповідного приміщення підвищений інтерес зловмисників; можлива шкідливість досить потужного джерела випромінювання для здоров'я людини; за певних умов метод не забезпечує гарантований захист комп'ютерної інформації [2].

Пасивний метод передбачає екранування джерела випромінювання технічного засобу, тобто засіб обчислювальної техніки розміщується в екранованій шафі або в цілком екранованому приміщенні. Тобто екранується кожний технічний засіб, що входить до складу наших засобів обчислювальної техніки. Як недолік такого методу можна виділити високу вартість екранованого приміщення, якщо мова йде про декілька засобів обчислювальної техніки [2].

Для того, щоб приховати джерело випромінювання, застосовується сучасна технологія, що базується на нанесенні (наприклад, розпилення) на внутрішню сторону існуючого корпусу и саме тому зовнішній вигляд комп'ютера фактично не зміниться. Навіть за сучасних технологій захист комп'ютера є складним процесом. Отже, захист комп'ютера здійснюється в кілька етапів: 1) спочатку здійснюються спеціальні роботи для зібраного комп'ютера, де визначаються частоти, їх рівні, на яких присутній інформативний сигнал; 2) далі йдуть етапи аналізу конструктивного виконання комп'ютера, розробки технічних вимог, вибору методів захисту, розробки технологічних рішень і розробки конструкторської документації для даного конкретного виробу (або партії однотипних виробів); 3) після проходження перших двох етапів, виріб надходить власне у виробництво, де і виконуються роботи по захисту всіх елементів комп'ютера; 4) після цього повинні бути проведені спеціальні випробування для підтвердження обгрунтованості рішення. У разі успішного проходження випробувань, замовникові буде видано відповідний документ, у якому зазначено, що даний комп'ютер є захищеним від витоку інформації по каналах електромагнітного випромінювання [3].

Отже, на підставі вищевикладеного очевидно, що розробляються засоби захисту від витоку електромагнітними каналами, є необхідними для забезпечення безпеки інформації.

Список використаної літератури:

1. Ярутич А. О. Захист інформації від витоку технічними каналами. *Наука Онлайн*. 2019. № 1.

2. Артем'єва А. В. Захист інформації від витоку по електромагнітним каналам. *Сенергія наук*. 2019. № 33. С. 1006–1012.

3. Кірєєва Н. В. Виток інформації по каналам ПЕМВ та способи її захисту. *Міжнародний журнал прикладних та фундаментальних досліджень*. 2016. № 8. С. 499–504.

Ключові слова: електромагнітні канали, конструкторсько-технологічні рішення, заземлення, екранування.

Ключевые слова: электромагнитные каналы, конструкторско-технологические решения, заземление, экранирование.

Keywords: electromagnetic channels, design and technological solutions, filtration, grounding, shielding.

Науковий керівник: *к.т.н. доц. Кухаренко С. В.*

Сафонов Камиль Муханнадович
Национальный университет «Одесская юридическая академия»,
студент 2 группы факультету кибербезопасности
и информационных технологий

ЗАЩИТА УСТРОЙСТВ КОММУНИКАЦИИ ПОЛЬЗОВАТЕЛЯ ОТ RAT ВИРУСОВ

В современном мире актуализирована проблема вирусного поражения цифровых устройств пользователей. К их числу относятся самые опасные шпионские RAT вирусы (Remote Access Trojan – Троян удаленного доступа) [1].

Алгоритм работы этого вируса позволяет злоумышленнику получить полный удаленный доступ к устройству пользователя жертвы, а следовательно к его файлам, личным данным, видеокамере, геолокации, данным банковских карт и т.д.

Структурно, RAT вирус состоит из двух частей: клиентской и серверной. С помощью клиентской части, которая установлена на устройство злоумышленника, и серверной, которую, ничего не подозревая, запускает пользователь на своем устройстве коммуникации. После запуска серверной части RAT вируса, на устройстве коммуникации пользователя, в клиентской части