РАЗДЕЛ I. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Аштаева Н.В.

Исследование технических каналов утечки информации

Волгоградский государственный университет
(Россия, Волгоград)

doi: 10.18411/lj-01-2021-01

idsp: ljjournal-01-2021-01

Аннотация

Статья посвящена вопросам защиты информации от утечки по техническим каналам. Изучается физическая природа возникновения информационных сигналов. Производится обзор и анализ возможных технических каналов утечки информации. Определяется вероятность утечки информации по различным техническим каналам.

Ключевые слова: информация, каналы утечки, техническая защита, технические средства, вспомогательные технические средства и системы (ВТСС), технические средства приема информации (ТСПИ).

Abstract

The article is devoted to the protection of information from leakage through technical channels. The physical nature of the occurrence of information signals is studied. The review and analysis of possible technical channels of information. The probability of information leakage through various technical channels is determined.

Keywords: information, leakage channels, technical protection, technical means, auxiliary equipment and systems, technical means of receiving information.

Введение

Актуальность данной темы заключается в том, что в основе любой деятельности человека лежит ее информационная поддержка. Информация становится одним из основных средств решения проблем и задач государства, политических партий и деятелей, различных коммерческих структур и частных лиц. Поскольку получение информации путем проведения собственных исследований становится все более дорогостоящим, расширяется сфера получения информации более дешевым, но незаконным способом. Этому способствуют недостатки нормативно-правовой базы защиты интеллектуальной собственности, позволяющей злоумышленникам (нарушителям законов) избежать серьезного наказания за свои противоправные действия, а также наличие на рынке различных технических средств незаконной добычи информации.

В связи с этими обстоятельствами актуальность задач защиты информации во всех сферах человеческой деятельности постоянно возрастает: на государственной службе, в бизнесе, в научной деятельности и даже в личной жизни. Постоянная конкуренция между методами и средствами получения и защиты информации, привела к появлению на рынке такого разнообразия устройств в этой области, что возникла проблема рационального выбора и применения защитных мер для конкретных условий.

Среди мер защиты информации все большее значение приобретает инженерно-техническая защита информации, основанная на использовании различных технических средств обеспечения информационной безопасности.

В частности, имитационное моделирование технических каналов утечки информации позволяет правильно определять приоритеты защиты и способы их достижения на ранней стадии планирования системы безопасности.

Анализ существующих каналов утечки информации

При выявлении каналов утечки технической информации (ТКУИ) все технические средства необходимо рассматривать как систему, включающую в себя основное (стационарное) оборудование, клеммы, соединительные линии (набор проводов) и кабели, проложенные между их частями), распределительные и коммутационные устройства, системы электроснабжения, системы заземления.

Отдельные технические средства или комплекс технических средств, предназначенных для обработки конфиденциальной информации, вместе с помещениями, в которых они расположены, являются предметом технических средств передачи информации (ТСПИ).

Вместе с ТСПИ в помещениях устанавливаются технические средства и системы, которые непосредственно не участвуют в обработке конфиденциальной информации, но используются совместно с ТСПИ и находятся в зоне действия создаваемого ими электромагнитного поля. Такие технические средства и системы называются вспомогательными техническими средствами и системами (СУДС). К ним относятся: технические средства открытой телефонной связи, громкой связи, пожарной и охранной сигнализации, электрификации, радио, часов, электроприборов и др.

Наиболее вероятна утечка информации по ВТСС, с выходом за пределы контролируемой зоны - территории, в которой появление людей и транспортных средств, не имеющих права доступа на территорию ТСПИ.

Для получения информации, обрабатываемой техническими средствами, заинтересованные в получении этой информации могут использовать широкий арсенал портативных средств технического распознавания (ТСР).

В зависимости от физической природы появления информационных сигналов, а также способов их распространения и способов перехвата технические каналы утечки информации можно разделить на электромагнитные, электрические и параметрические.

Анализ существующих методов защиты каналов утечки информации

Для создания системы защиты объекта от утечки информации по техническим каналам необходимо предпринять ряд мер. В первую очередь, это анализ конкретных особенностей расположения построек и содержащихся в них помещений, территории вокруг объекта и подключенных к ним коммуникаций. Поэтому необходимо выбрать те помещения, в которых распространяется конфиденциальная информация, и учесть используемые в них технические средства. Далее необходимо провести следующие технические мероприятия:

- проверить используемую технику на соответствие величины побочных излучений допустимым уровням;
- экранировать помещения с техникой или эту технику в помещениях;
- перемонтировать отдельные цепи, линии, кабели;
- использовать специальные устройства и средства пассивной и активной защиты.

Моделирование технических каналов утечки информации

При выявлении технических каналов утечки информации необходимо учитывать весь набор защитных элементов, включая основное оборудование технических средств обработки информации, оконечные устройства, линии связи, распределительные и коммутационные устройства, системы электроснабжения, системы заземления и тому подобное. Помимо наиболее важных технических средств, непосредственно связанных с обработкой и передачей конфиденциальной информации, необходимо учитывать технические средства и системы, например, технические средства для открытых телефонов, факсов, громкой связи, охранной и пожарной сигнализации, электрификации, радиосвязи, бытовой техники и др. В качестве каналов утечки интерес представляют вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода и кабели, к ним не относящиеся, но проходящие

через помещения, где установлены основные и вспомогательные технические средства, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

При моделировании каналов технической утечки необходимо, прежде всего, выявить сами каналы утечки информации (источник сигнала и пути утечки), а затем оценить реальность канала, масштаб и ранг угрозы. Оценка реальности угрозы определяется как отношение стоимости информации к стоимости реализации канала утечки, а величина угрозы определяется как произведение цены информации и вероятности реализации канала.

Для моделирования используются следующие понятия:

1. Пропускная способность канала утечки информации;

Определяется, например, для средств акустического контроля:

$$C_0 = F \cdot \log_2(1+q) \quad , \quad (1)$$

где C_0 – пропускная способность канала;

ΔF – ширина частотной полосы сигнала;

q – соотношение сигнал/помеха по мощности

2. Стоимость элемента информации:

$$C_{\text{и}} = C_0 \cdot t \cdot C_{\text{э}} \quad , \quad (2)$$

где C_0 – пропускная способность канала утечки информации;

t – время работы канала;

$C_{\text{э}}$ – стоимость 1 Кбайта элемента информации.

3. Оценка реальности канала утечки информации:

$$\alpha = \frac{C_{\text{и}}}{C_{\text{ку}}} \quad , \quad (3)$$

где $C_{\text{и}}$ – стоимость элемента информации;

$C_{\text{ку}}$ – стоимость канала утечки информации.

4. Величина угрозы:

$$C_{\text{у}} = C_{\text{и}} \cdot \alpha \quad , \quad (4)$$

где $C_{\text{и}}$ – стоимость элемента информации;

α - оценка реальности канала утечки информации.

Также необходимо произвести классификацию имеющейся информации по принципу важности.

После вычисления всех параметров каждого технического канала утечки информации составляется сводная таблица, пример которой приведен в таблице 1.

Таблица 1

Сводная таблица параметров технических каналов утечки информации

вид информации	цена информации	источник утечки	путь утечки	вид канала утечки	вероятность утечки
Сведения о договорных обязательствах	12000	ПЭМИН телефона	телефонная закладка	электрический	0,4
		ПЭМИН монитора	сканирование селективным вольтметром	электрический	0,09
		ПЭМИН питающего кабеля	сканирование селективным вольтметром	электрический	0,3
		акустические волны (разговор)	направленный лазерный микрофон	оптоэлектронный	0,7
		акустические волны (разговор)	акустическая закладка	акустический	0,5

В таком порядке необходимо оценить вероятность утечки по каждому техническому каналу каждого вида информации. На основании систематизации этих данных должно приниматься решение о необходимых элементах системы безопасности.

1. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности, СПб, Питер, 2008 г., 320 стр.
2. В. В. Домарев Безопасность информационных технологий. Системный подход, Издательство: ТИД "ДС", 2004 г., 992 стр.
3. Петраков А.В. Основы практической защиты информации. 3-е изд. Учебное пособие-М.: Радио и связь, 2001 г.-368 стр.
4. Бузов Г. А, Калинин С.В., Кондратьев А. В, Защита от утечки информации по техническим каналам, М. Горячая линия, Телеком, 2005 г, 416 стр.
5. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998 г. - 320 стр.
6. Торокин А. А. , Основы инженерно-технической защиты информации, книга 1, РГУ, 1997 г. - 267 стр.
7. Бабурин А.В., Чайкина Е.А., Воробьева Е.И. Физические основы защиты информации от технических средств разведки: Учеб. пособие. Воронеж: Воронеж. гос. техн. ун-т, 2006 г.-193 стр.

Байчорова К.Т.

Цифровой прогресс и его влияние на современное общество

*Северо-Кавказская государственная академия
(Россия, Черкесск)*

doi: 10.18411/lj-01-2021-02

idsp: ljjournal-01-2021-02

Аннотация

В статье раскрывается проблема того, к каким последствиям может привести цифровая трансформация, положительные и отрицательные стороны прогресса, а также отрасли, в которых он будет происходить в ближайшее время.

Ежедневно период времени, в течение которого человек находится в сети в течение дня, увеличивается. Активное использование потенциала сети имеет как положительные, так и отрицательные последствия. Цифровые компетенции, которые включают цифровое потребление и цифровую безопасность, имеют большое значение в информационном обществе.

Ключевые слова: цифровизация, образовательная среда, цифровой прогресс, общество.

Abstract

The article reveals the problem of what consequences digital transformation can lead to, the positive and negative aspects of progress, as well as the industries in which it will occur in the near future. Every day, the period of time that a person is online during the day increases. Active use of the network's potential has both positive and negative consequences. Digital competencies, which include digital consumption and digital security, are of great importance in the information society.

Keywords: digitalization, educational environment, digital progress, society.

Цифровизация – это тот новый аспект развития современного мира, от которого обычному человеку будет очень сложно абстрагироваться. Это то, с чем невозможно бороться и остается лишь идти в ногу со временем. Информационные технологии настолько сильно влились в нашу жизнь, что уже невозможно представить себе место где не было бы интернета, систем электронных платежей и иных цифровых новшеств.