Мальсагова Вероника Сергеевна
студентка
Научный руководитель
Фомичева Татьяна Леонидовна
канд. экон. наук, доцент
ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Москва

О СРЕДСТВАХ ЗАЩИТЫ ЦИФРОВОЙ И АНАЛОГОВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Аннотация*: в работе проведен обзор средств и действий по защите цифровой и аналоговой информации, которые производятся для обеспечения информационной безопасности. Описываются концептуальные основы технической защиты информации, классифицируются ее основные принципы, определяются основные методы и средства обеспечения информационной безопасности от возможных вариантов утечки информации.*

Ключевые слова*: Ключевые слова: безопасность, информация, защита, утечка, технические каналы.*

Введение.

Потеря информации по техническим каналам является одной из основных угроз безопасности ограниченной информации, связанной с неконтролируемым распространением информационного сигнала от источника по физическому носителю на техническое устройство, которое получает информацию. Перехват информации – это незаконное получение информации с использованием технических средств, которые обнаруживают, получают и обрабатывают информационные сигналы. В результате перехвата информации возможно незаконное ознакомление с информацией или незаконная запись информации на носитель.

Причины утечки информации.

Наиболее распространенные причины потери информации включали недостаточную защиту данных других людей (от организации или от прокси-сервера) и неадекватное управление устройствами, которые хранят информацию (по техническим причинам). Все это происходит при сопутствующих условиях, которые допускают ситуацию потери [2]:

– некомпетентность сотрудников, занимающихся защитой данных, их непонимание важности процесса и их небрежное отношение к информации в целом;

– использование нелицензионных средств или несертифицированных программ для защиты и сохранения конфиденциальности клиентов;

– низкий уровень контроля над средствами по охране сведений;

– постоянная смена сотрудников, занимающихся защитой персональных данных.

Вину за утечку информации, как правило, несут сотрудники фирм и компаний, а также их руководители. Вы можете защитить себя от любых вторжений, если хотите, и от некомпетентности сотрудников. Существуют также факторы, независимые от компаний, такие как масштабные бедствия, стихийные бедствия, аварии на технических станциях и отказы оборудования.

Технические каналы утечки информации.

Технический канал утечки информации – совокупность источника информации, линии связи (физической среды), через которую передаются информационные сигналы, шумы, препятствующие передаче сигнала по линиям связи, и технических средств перехвата информации.

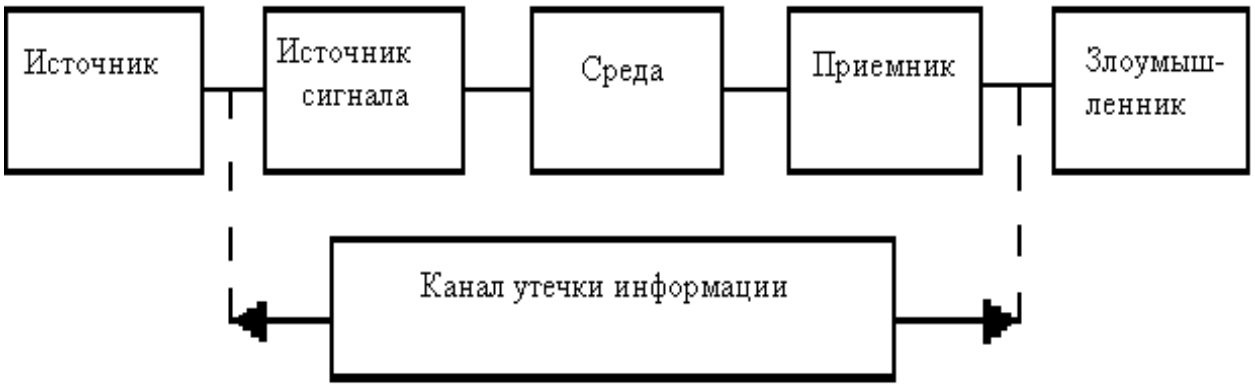

Рис. 1

По причине возникновения различают:

– естественные ТКУ (к ним относятся ТКУ, образовавшиеся из-за несовершенства конструкторских и технологических качеств технических средств хранения, обработки и передачи информации);

– искусственно созданные ТКУ (намеренно организованные, обычно посредством внешних энергетических воздействий на носитель или коммуникацию).

Характеристики каналов утечки технической информации определяются физической природой информационных сигналов и характеристиками среды распространения. Канал утечки информации включает в себя передатчик, реальный канал и приемник. Эмитент относится к произвольному источнику защищенной информации, независимо от формы его существования. Это может быть тип технического инструмента, человеческий язык и т. Д. Канал, как правило, представляет собой тип физической среды, в которой распространяется сигнал передатчика. Канал утечки имеет две основные характеристики: удельное демпфирование и определенный уровень шума. Реализация такого обобщенного канала может быть твердым телом (стенка, труба), проводной линией, пространством (для электромагнитной волны), воздухом и т д. Получатель этой модели является потенциальным противником, а также технические средства для перехвата информации (с или без) вас).

Сигналы несут соответствующую информацию. По своей природе сигналы могут быть акустическими, электромагнитными, электрическими и другими типами вибраций (волн), и информация содержится в изменениях их параметров. В зависимости от характера сигналов они распространяются в определенных физических средах. Основным средством распространения является воздух, твердые и жидкие среды. Средства перехвата информации используются для приема и преобразования сигналов с целью получения информации [3].

Общая классификация технических каналов утечки информации включает в себя следующие типы каналов (рис. 2):

– каналы утечки, которые обрабатываются техническими средствами приема, обработки, хранения и передачи информации;

– каналы утечки голосовой информации;

– каналы утечки информации при передаче по каналам связи;

– технические каналы утечки видовой информации.

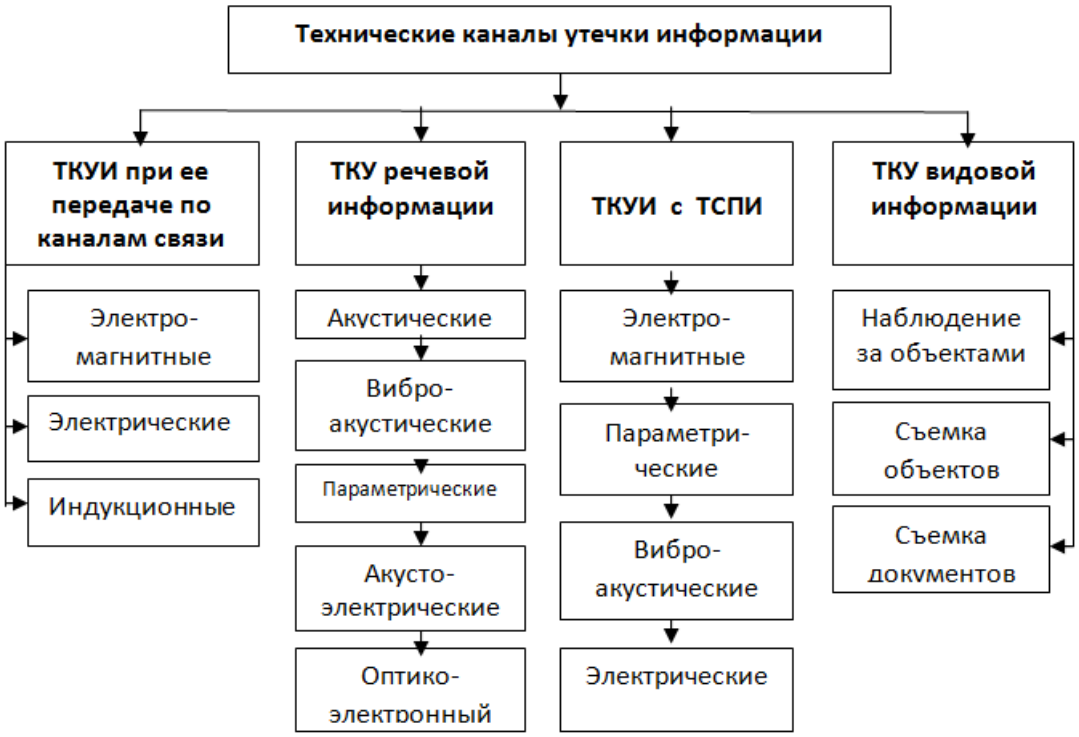

Рис. 2. Общая классификация технических каналов утечки информации

Сегодня существуют технические средства, которые рискуют сформировать технический канал для передачи информации. Все данные на устройстве хранятся в электронном и зашифрованном виде. На самом устройстве все части (узлы, проводники и другие элементы) могут генерировать волны с их частотой и, таким образом, распространять данные по техническим каналам утечки информации. Следует отметить, что мошенники чаще всего используют акустические и электромагнитные каналы утечки, поскольку они менее заметны и надежны при сборе информации. Самый быстрый способ захвата аудиоинформации.

Есть несколько способов, которыми мошенники используют для извлечения информации. Это технические средства, они работают в разных процессах, но в

большинстве случаев эффективно. Все средства разделены на пассивы и активы. Среди них наиболее популярными являются:

– режимные АТС;

– электронно-вычислительные техника;

– системы оперативно-командной и громкоговорящей связи;

– устройства усиления звука и звукозаписи.

К активным средствам можно отнести такие моменты:

– незаконное вклинивание или подключение к каналам, кабелям или линиям связи;

– высокочастотное наложение;

– механическая установка канала утечки на микрофоны и телефоны.

Способы защиты информации от утечки по техническим каналам.

Защита информации от утечки через визуально-оптический канал представляет собой комплекс мер, исключающих или уменьшающих вероятность того, что конфиденциальная информация покинет контролируемую зону из-за распространения световой энергии. Используя визуальную систему, человек получает наибольшее (до 90%) количество информации из внешнего мира. Смежные видимые области (инфракрасные и ультрафиолетовые) также содержат важную информацию об окружающих объектах, но не могут быть непосредственно видны человеческому глазу. Для этого используются различные типы преобразования невидимого изображения в видимое изображение – визуализация невидимых изображений. Уменьшение освещения приводит к ухудшению зрения и, как следствие, к уменьшению диапазона и низкой цветопередаче. Эти физические характеристики необходимо учитывать при защите информации от утечки по визуально-оптическим каналам. Рекомендуется защищать информацию от утечек через визуально-оптический канал [4]:

– размещение объектов защиты так, чтобы предотвратить отражение света в направлениях возможного расположения злоумышленника (пространственные ограждения);

– уменьшить отражающие свойства защитного объекта;

– уменьшить освещение защитного объекта (энергетические ограничения);

– использовать средства затруднения или значительного ослабления отраженного света: ширмы, экраны, шторы, ставни, темные стекла и другие средства затруднения;

– использовать маскирующие, имитационные и другие средства для защиты и обмана злоумышленника;

– использовать средства пассивной и активной защиты источника от неконтролируемого распространения отражающего или излучаемого света и других излучений;

– маскировать защитные объекты, изменяя отражающие свойства и контрастность фона.

Методы защиты информации в радиоканале можно разделить на две группы:

– ограничение физического доступа к линии и коммуникационному оборудованию;

– преобразование сигналов в линии к форме, которая исключает восприятие или искажение содержимого передачи для злоумышленника.

Заключение.

Во избежание потери информации техническими средствами после установки и внедрения технических средств защиты информации их экспериментальные операции выполняются в сочетании с другим аппаратным и программным обеспечением для проверки их работоспособности в контексте средств компьютеризации. и разработка технологического процесса обработки информации (передачи). Кроме того, во время работы следует регулярно проводить специальные проверки и аудиты специализированных кабинетов и агентов по компьютеризации. Специальные расследования должны проводиться в отсутствие персонала организации (допускается ограниченная группа руководителей и сотрудников службы безопасности) [5].

Важно уделять достаточное внимание защите от подключения внешних технических каналов утечки. Появление технических каналов для утечки

информации не является редкостью, поэтому важно знать больше, чтобы защитить себя и свою конфиденциальность в разговорах или при отправке сообщений.

Список литературы

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) // Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России).

2. Утечки информации [Электронный ресурс]. – Режим доступа: https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/

3. Техническая защита информации / Национальная библиотека им. Н.Э. Баумана.

4. Ворона В.А. Концептуальные основы создания и применения системы защиты объектов: учебное пособие. Кн. 1 / В.А. Ворона, В.А. Тихонов. – М.: Горячая линия – Телеком, 2012. – 184 с. (Серия «Обеспечение безопасности объектов»).

5. Доктрина информационной безопасности Российской Федерации (принята 9 сентября 2000 г. №ПР-1895).