Информация может быть представлена в различной форме и может храниться на различных физических носителях.

Документальная информация содержится в графическом и буквенно-цифровом виде, а также в форме электронных документов, на магнитных и других носителях.

Речевая информация возникает в ходе ведения разговоров, а также при работе систем звукоусиления и звуковоспроизведения.

Телекоммуникационная информация циркулирует в технических средствах обработки и хранения информации, а также в каналах связи.

Необходимость совершенствования средств физической защиты различных носителей информации является одной из главных задач любого объекта, будь то отдельно взятый индивид, или же некоторая организация. По статистике, главным источником утечки информации является человек. Для получения злоумышленником информации используются:

- сознательные действия сотрудников, обусловленные инициативным сотрудничеством с другой фирмой; продажей информации за взятку, под угрозой шантажа, в виде мести; переход на другую фирму на более высокую оплату (так называемая «кража мозгов»);
- обман (например, за счет создания ложной фирмы, в которую заманивают специалиста на собеседование, беседуют, выуживают сведения и затем отказывают в приеме);
- особенности характера сотрудника, например, его болтливость, желание показать себя более компетентным;
- слабое знание и невыполнение требований по защите информации и т. д. [3, с. 20]

Документы и публикации являются также одним из важных возможных каналов утечки информации. Для уменьшения возможности утечки информации руководство организации предпринимает следующие действия:

- разработка перечня документов с грифом «Коммерческая тайна» (этот термин обозначает информацию, которая позволяет получать предприятию большую

прибыль по сравнению с конкурентом);
- уточнение списка лиц, допускаемых к работе с документами;
- организация учета входящих, исходящих документов и правил работы с ними;
- определение правил уничтожения документов [1, с. 35].

Для обеспечения технической деятельности компании или организации широко используются телефоны, радиотелефоны, компьютеры, принтеры, дисплеи, клавиатура, обычный речевой обмен информацией и т. д. Для нелегального съёма информации используются различные технические средства. Информация с объекта поступает злоумышленнику по следующим физическим каналам: акустическим каналам; вибрационному каналу колебаний конструкций здания; электромагнитным каналам; телефонным каналам; электросетевым каналам; визуальным каналам.

В общем виде под техническим каналом утечки информации понимают совокупность 1) источника опасного сигнала, 2) среды распространения – носителя опасного сигнала, 3) средства технической разведки [2, с. 23].

Перехват информационных сигналов по электрическим каналам утечки возможен путём непосредственного подключения к соединительным линиям вспомогательных технических средств и систем (это информационные системы, размещенные в помещениях обработки конфиденциальной информации) и посторонним проводникам. Для этих целей используют специальные средства радио- и радиотехнической разведки, а также специальная измерительная аппаратура [3, с. 89].

Вибрационные каналы утечки информации формируются на основе элементов конструкции здания. Такие способы используются наиболее редко из-за низкой надежности получения несанкционированной информации. Канал является собирательным понятием, участие в его формировании принимают стены здания, система водоснабжения и канализации, трубы, полы, потолки. В качестве устройств для считывания используются лазерные системы, электронные стетоскопы, специальные преобразователи шумов [1, с. 103].

Сложнее всего определить, есть ли такой канал утечки информации с предприятия или нет. Опасность заключается в том, что подобным способом можно получить информацию сразу с нескольких типов носителей. А закрыть этот путь утечки и защитить данные можно с помощью системы виброакустического зашумления. Помехи, создаваемые таким устройством, подаются на усилитель мощности, а

затем сигнал поступает на акустический вибратор. После включения устройства появляются колебания стен, которые подавляют передачу информации из помещения.

Акустические каналы утечки информации. В воздушных (прямых акустических) технических каналах утечки информации средой распространения акустических сигналов является воздух.

Для перехвата акустической (речевой) информации используют следующие устройства:

- портативные диктофоны и проводные микрофонные системы скрытой звукозаписи;
- направленные микрофоны;
- акустические радиозакладки (передача по радиоканалу) и др. [3, с. 230].

Данный канал утечки не имеет деконспирационных признаков, и, следовательно, представляется затруднительным технически определить, происходит ли утечка информации по этому каналу [2, с. 221]. Специалисты осуществляют оценку возможности утечки информации на основании изучения архитектурно-строительной документации на определенную часть объекта с последующей проверкой выводов с помощью стетоскопов. Если оказывается, что такой канал утечки возможен, то встаёт задача закрытия этого канала.

Примеры:

1. 28 января 2020 года стало известно об утечке данных клиентов сети алкомаркетов «Красное и Белое». В интернет попала база программы лояльности.

Как пишут «Ведомости», с сентября 2019 года на форуме «Дубликаты» продавалась часть базы с данными о 124 тыс. человек. За нее просили 15 тыс. рублей, а потом она стала доступна для скачивания всем желающим. База постоянно пополнялась. В конце января база с данными на 2 млн человек появилась на форуме «Фрикер клуб», и на 4 млн — на англоязычном форуме Raid [6].

1. 5 ноября 2019 года стало известно о том, что данные около 3,5 тыс. клиентов «Альфа-банка» и около 3 тыс. клиентов «АльфаСтрахования» выставлены на продажу. Соответствующее объявление было обнаружено на одном из

специализированных форумов.

Как пишет РБК, база содержит ФИО, номер мобильного телефона, данные паспорта и регистрации, сумма кредитного лимита или страховки, предмет и дата страхования. Все договоры «Альфа-банка» были оформлены в октябре, а страховки — 8 мая 2019 года, утверждает продавец.

Чтобы проверить подлинность данных, продавец предлагает потенциальным покупателям ознакомиться с 23 договорами. Журналисты проверили эти документы. При попытке перевести деньги по указанным номерам телефонов, инициалы получателя совпали с указанными в договорах в 11 из 13 случаев. При этом данные клиентов «АльфаСтрахования» не подтвердились.

Один из клиентов «Альфа-банка» рассказал изданию, что ему уже позвонили мошенники, и он заблокировал карту.

В «Альфа-банке» РБК подтвердили утечку персональных данных, но заявили, что она коснулась лишь 15 клиентов. Также в банке заверили, что случившееся не угрожает средствам на счетах. Однако банк все равно проводит расследование, чтобы определить масштаб проблемы и устранить причины утечки [5].

1. В начале апреля 2020 года стало известно о появлении в даркнете данных более 500 тыс. учетных записей Zoom, которые были выставлены на продажу. Эти данные содержат адреса электронной почты, пароли, URL-адреса для организации закрытых встреч, а также идентификаторы персональной конференции (цифровой код, который используется в определенных случаях).

Опубликованные данные позволяют хакерам «зумбордировать» — это форма троллинга, при которой злоумышленник помещает в чужие видеоконференции Zoom произвольный контент, чаще оскорбительного характера. За последнее время под прицелом троллей оказались виртуальная синагога, женское сообщество и клуб анонимных алкоголиков.

Так, при атаке на клуб анонимных алкоголиков злоумышленники вставили в видеовстречу закадровый голос со словами: «Выпивка — это так прекрасно», а при атаке на синагогу — оскорбительные антисемитские высказывания.

Компания Cyble, специализирующаяся на кибербезопасности, сообщила, что ей удалось договориться с хакерами о приобретении данных приблизительно 530 тыс. аккаунтов по цене $0,002 за один аккаунт ($1,6 тыс. за всю базу). Многие учетные

записи принадлежат организациями, включая Citibank, Chase и различные учебные заведения. При этом, как выяснилось, на некоторых форумах часть украденных данных предлагалась и вовсе бесплатно [4].

Обеспечение конфиденциальности информации – одна из основных и наиболее сложных задач, которые необходимо решать каждому предприятию. Сегодня организация работы любого предприятия, будь оно частным или государственным, претендующего на успешное развитие, обязательно базируется на современных информационных технологиях. Поэтому необходимо обращать внимание на стандарты управления информационной безопасностью. Как правило, вопросы управления информационной безопасностью тем актуальнее, чем крупнее организация, чем шире масштаб ее деятельности и претензии на развитие, и, как следствие, выше ее зависимость от информационных технологий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Богатырев, В. А. Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — Москва : Издательство Юрайт, 2020. — 318 с.
2. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с.
3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с.
4. Researchers found and bought more than 500,000 Zoom passwords on the dark web for less than a cent each / Иrsiness Insider, 2020. URL: https://www.businessinsider.com/500000-zoom-accounts-sale-dark-web-2020-4
5. Данные клиентов Альфа-банка утекли в Сеть / РБК, 2019. URL: https://www.rbc.ru/finances/05/11/2019/5dbc07929a7947c6597cf70f
6. В интернете опубликована база данных клиентов сети алкомаркетов «Красное и белое» / Газета "Ведомости", 2020. URL: https://www.vedomosti.ru/business/articles/2020/01/27/821576-baza-klientov