УДК 004.056 EDN COJPAU

Каналы утечки информации и технические средства её хищения

Н.О. Гадючный*

Новосибирский государственный технический университет, пр-т. К. Маркса, 20, Новосибирск, 630073, Россия

*E-mail: abt.soul@mail.ru

Аннотация. Рассмотрены основные каналы утечки информации, также технические средства ее хищения. Выделены основные группы каналов утечки информации: материально-вещественные, визуальные и технические. Приведены примеры хищения используя различные каналы. А также рассказаны простейшие и понятные способы защиты личной информации от ее утечки.

Ключевые слова: каналы утечки, хищение информации, утечка личной информации

Channels of information leakage and technical means of its theft

N.O. Gadyuchnyj*

Novosibirsk State Technical University, 20 K.Marks pr., Novosibirsk, 630037, Russia

*E-mail: abt.soul@mail.ru

Abstract. The main channels of information leakage, as well as technical means of its theft, are considered. The main groups of information leakage channels are singled out: tangible, visual and technical. Examples of theft using various channels are given. And also the simplest and most understandable ways to protect personal information from leakage are described.

Keywords: leakage channels, information theft, personal information leakage

1. Введение

С течением времени технологии все больше и больше занимают место в нашей жизни. Большая часть информации переводится в электронный вид, записывается на различные устройства хранения или сохраняется во всемирной сети «Интернет». При всем этом люди специалисты стараются обеспечить должный уровень защиты вашей личной информации и предотвратить ее распространение третьим лицам. Но не всегда это удается сделать так как злоумышленники также развиваются и придумывают все более сложные схемы хищения информации. Они пользуются социальной инженерией и другими способами получения конфиденциальной информации. Такие атаки необходимо отлеживать, собирая по крупицам полный объем атаки, отслеживать отдельные инциденты и анализировать их совокупность. Чтобы не попасться на удочку мошенников нужно быть осведомленным о каналах, способах и средствах хищения информации.

Каналы утечки информации существуют в любом информационном пространстве. Под каналом утечки в самом общем смысле понимается неконтролируемый способ передачи информации. В результате злоумышленник может получить несанкционированный доступ к нужным ему конфиденциальным данным компании.

2. Основные группы каналов утечки информации

По результатам анализа зарегистрированных утечек информации за 9 месяцев 2020 года (проведенным авторитетным аналитическим центром при поддержке компании «Ростелеком») выделяют 3 основных группы каналов:

1. Материально-вещественные
2. Визуальные и визуально-оптические
3. Технические

Чаще всего хищение информации по утверждению центра происходит через технические каналы утечки и одна из причин этого заключается в том, что это самая многочисленная группа. Однако не стоит забывать и про первые две группы так как они получают все большее развитие в последнее время.

Рассмотрим каждую группу по очереди, включая советы по защите данных в данной группе каналов [1].

2.1 Материально-вещественные каналы: примеры и меры защиты информации от утечек

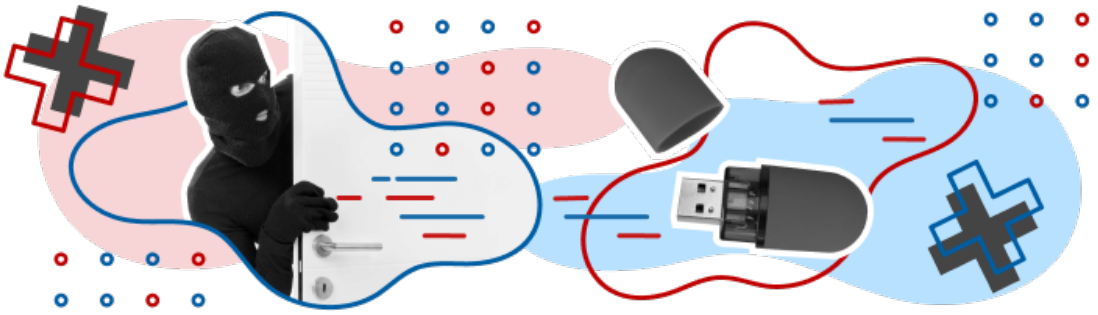

Рисунок 1. Иллюстрация 1.

О данном канале можно говорить в случае утечки информации в результате хищения физического носителя информации или копирования его содержимого с помощью различных технических устройств без согласия владельца данного носителя. То есть в данном случае говорится о непосредственном физическом контакте злоумышленника с носителем.

Примером таких инцидентов может послужить:

- Передача или отправка физических документов
- Хищение или потеря USB-накопителя

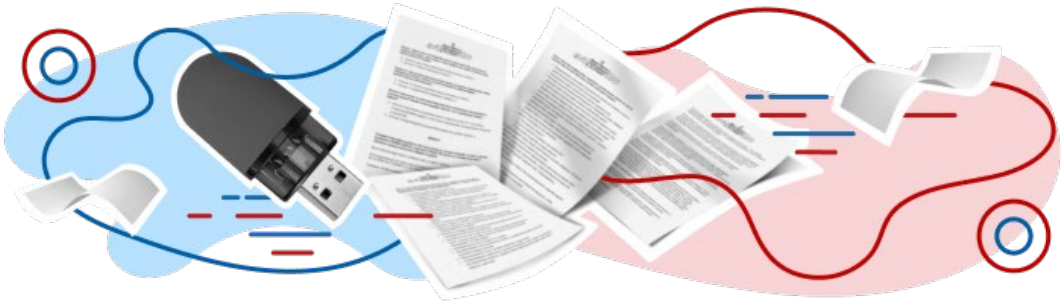

Рисунок 2. Физические носители информации.

Способы защиты для данного канала делятся на две группы: организационные и технические.

Организационные меры предполагают внедрение системы учета физических документов и носителей информации, также различные допуски к ним, принтерам и любой другой копировальной технике. А также самым простым и банальным способом защиты в данном канале является простая внимательность и осторожность с физическими документами и носителями информации.

Что касается технических мер, то самым эффективным способом защиты при хищении ее носителя – это использование средств шифрования данных, которые хранятся на нем с помощью различных алгоритмов (например AES-256, BlowFish-448 и им подобных). В таких случаях есть вероятность, что даже при краже вашего носителя, ваши данные не достанутся злоумышленникам [2].

2.2 Визуальные и визуально-оптические каналы утечки информации

Данный канал характеризуется самыми банальными способами хищения информации, так как основные способы утраты информации возникают при дистанционном считывании и фиксации информации с различных носителей: например, фотографирование дисплеев мониторов, экранов для демонстрации презентаций, бумажных носителей, оставленных без присмотра, аудиозапись переговоров и подобные. Непосредственно физического контакта с носителем данных в этом случае не происходит.

Примеры таких хищений также банальны:

- Фото оставленных или выкинутых документов
- Фото или видеозапись личной информации с экрана монитора

Рисунок 3. Пример хищения информации используя визуально-оптический канал.

Для защиты информации от утечки по этому каналу специалисты по защите информации рекомендуют выполнять следующие действия:

- Применять маскировку объектов и носителей информации. Технологий масса — от управления контрастом фона, на котором демонстрируется защищаемая информация, до применения аэрозольных завес и других специальных решений.
- Располагать экраны и другие защищаемые объекты так, чтобы исключить отражение света в сторону посторонних лиц.
- Оборудовать помещения, в которых работают с визуальными данными, средствами преграждения или ослабления отраженного света: темными стеклами, шторами, роллетами, ставнями.
- Ограничивать доступ сотрудников к визуальной информации. В этом помогут специально разработанные политики безопасности [3].

2.3 Основные технические каналы утечки информации

Технические каналы утечки информации возникают при обработке и передаче данных в технической среде и по каналам связи, также при несанкционированном доступе к ним с ним помощью устройств, программного обеспечения или аппаратно-программных комплексов для скрытого получения информации.

Все это из-за того, что обмен информацией сегодня происходит чаще всего при использовании телефонной связи, компьютера и других электронных средств.

Согласно анализу центра, основные технические каналы утечки информации, следующие:

- Мобильные устройства. Увеличение гибридной работы из-за Covid-19 означает, что сотрудники обмениваются большим количеством разговоров и документов через приложения для обмена сообщениями, такие как WhatsApp, WeChat, Signal, Telegram и LINE. Эти разговоры стали новым каналом, который ИТ-отделы должны учитывать в своих программах предотвращения потери данных.
- Электронная почта. Чаще всего по этому каналу происходят инсайдерские утечки. Для предотвращения таких случаев используются фильтры для запрета отправки почты на определённые адреса и домены. Также возможна установка системы анализа содержимого писем и прикрепляемых вложений. Ну и на конец проверять адреса отправителя и получателя. Для дополнительной защиты информации в

подобных случаях целесообразно использовать шифрование сообщений. Даже если данные попадут в третьи руки, расшифровать их будет проблематично.

- Сеть. Среди способов несанкционированного получения данных по сети существуют: прослушивание сетевых интерфейсов, подключение к сети технических устройств перехвата и использование вредоносного программного обеспечения (черви, вирусы и пр.). Но и вариантов защиты немало. Это: антивирусы, межсетевые экраны и комплексные решения, такие как IPS-, DLP-, IDS-системы иные средства [3].

3. Рекомендации по защите

Компании, работающие с конфиденциальной информацией любого типа, нуждаются в собственной комплексной системе безопасности, которая является барьером для злоумышленника на всех уровнях обработки данных.

Система защиты должна создаваться с учетом всех выявленных каналов утечки. В дальнейшем за поддержку автоматизированной системы защиты отвечает служба безопасности.

Факт кражи информации выявляется двумя основными способами. В первом случае сотрудник становится свидетелем происшествия и может рассказать о том, кем и как была украдена информация. В этом случае вероятность поймать вора всегда выше до того, как он передаст важные данные конкуренту. Важно не допустить, чтобы организация получила убыток, поэтому всегда стараются выявить инсайдера «по горячим следам».

Во втором сценарии факт кражи становится известен после того, как компания-конкурент использовала данные в своих целях. По этому сценарию события развиваются в подавляющем большинстве случаев. Факт кражи, о котором владелец информации не знал, произошел из-за использования злоумышленником дыры в безопасности или из-за отсутствия системы безопасности как таковой.

Утечка данных в первую очередь является результатом нарушения способа защиты конфиденциальных данных и основной причиной финансовых и «нематериальных» потерь компании. При выявлении утечки основная задача службы безопасности — как можно быстрее начать действия по выявлению злоумышленника.

Расследование проводится в рамках закона. Первый шаг — использовать организационные меры и закрыть доступ к данным, так как есть риск повторной кражи.

Далее следует начать разбирательство. На техническом уровне DLP-системы могут предотвращать утечки, автоматически обнаруживая попытку несанкционированной передачи информации за пределы защищаемой среды.

На первом этапе расследования служба безопасности определяет вид и способ утечки: случайная или спланированная. Как правило, факт потери по неосторожности или непреднамеренной утечки данных легко выявить на этапах анализа отчета DLP-системы, разговора с персоналом или после просмотра видеороликов.

В результате утечки информации компания может понести серьезные убытки. Ущерб может быть связан с различными причинами: кражей технологии изготовления изделия, кражей важных документов, разглашением секретной информации и т. д. Поэтому на этапе разработки системы безопасности следует учитывать все возможные пути хищения информации, через которые злоумышленник может получить доступ к защищенной информации.

4. Вывод

Единой для всех классификаций каналов утечки личной информации нет. Поэтому разные источники и разные специалисты выделяют свои особенности (учитывая специфику различных факторов и специфику их среды деятельности).

На самом деле не важна классификация каналов хищения информация, она в любом случае включает в себя все возможные каналы и пути хищения конфиденциальной информации. Поэтому не важно, как разделять и классифицировать средства утечки информации, необходимо выявлять все возможные пути их использования, а также своевременно принять меры к предотвращению таких случаев.

Список литературы

1. Основные каналы утечки информации [Электронный ресурс] URL: https://rt-solar.ru/products/solar_dozor/blog/2085/ (дата обращения 02.12.2022)
2. Кража данных и способы ее реализации [Электронный ресурс] URL: https://www.ptsecurity.com/ru-ru/research/knowledge-base/krazha-dannyh-i-sposoby-ee-realizacii/ (дата обращения 02.12.2022)
3. Защита от утечки конфиденциальной информации [Электронный ресурс] URL: https://www.azone-it.ru/zashchita-ot-utechki-konfidencialnoy-informacii (дата обращения 03.12.2022)

4. Main channels of information leakage [Электронный ресурс] URL: https://searchinform.com/challenges/information-security/information-security-analytics/information-leaks/information-leakage-causes/main-channels-of-information-leakage/ (дата обращения 23.02.2023)
5. Сборники конференций РИНЦ [Электронный ресурс] URL: https://na-konferencii.ru/conference-ref-cat/rints (дата обращения 23.02.2023)