**КАНАЛЫ УТЕЧКИ КОНФЕНДЕНЦИАЛЬНЫХ СВЕДЕНИЙ И МЕТОДЫ БОРЬБЫ С НИМИ**

**Чорненький Александр Александрович**

*Сотрудник Академии ФСО России*

**Аннотация:** В современном мире каждый собственник ценной или конфиденциальной информации старается защитить ее от различных методах доступа к ней и ее хищения. Существует множество каналов утечки информации, которые подразделяются по различным классификационным признакам. Цель собственника информации выявить  их защититься от  несанкционированного доступа.

**Ключевые слова:** технические каналы утечки информации, несанкционированный доступ, противодействие разведке.

Каналы утечки информации существуют в любом информационном пространстве. Канал утечки в самом общем смысле понимается как неконтролируемый способ передачи информации. В результате злоумышлен-ник может получить несанкционированный доступ к конфиденциальным данным компании, которые ему нужны.  
 К утечкам информации относятся:  
1) раскрытие данных теми, кто имеет доступ к секретной информации;  
2) потеря флэш-накопителей и других типов носителей данных, на которых хранилась конфиденциальная информация;  
3) преднамеренное хищение секретной информации с использованием шпионажа направленных на открытые каналы утечки информации.  
 Как правило, факт утечки конфиденциальной информации выявляется не сразу. В результате, например, получения коммерческой тайны предприятия конкурент может долгое время не выдавать себя и не распространять данные. Однако факт хищения "всплывает" со временем, что выражается в виде серьезных финансовых или материальных потерь для организации.  
 Согласно общепринятой классификации, существующие каналы утечки информации могут быть косвенными или прямыми. Когда речь заходит о косвенных каналах, это означает, что злоумышленник имеет прямой доступ к технической среде конкретной системы информационной безопасности.  
 Примеры косвенных утечек:  
1) потеря флэш-носителя или его преднамеренная кража;  
2) поиск конфиденциальных данных с помощью попыток исследовать мусор, выброшенные документы  и т.д;  
3) считывание паразитного электромагнитного излучения и помех;  
4) попытка кражи информации с использованием оптических средств: фотографирование объектов информационной системы, прослушивание помещений.  
 При взаимодействии с прямыми каналами злоумышленник получает доступ к оборудованию и информации, которая используется в информационной системе. Ярким примером прямого канала утечки является работа инсайдеров. Сами сотрудники компании в большинстве случаев становятся средством передачи информации злоумышленнику. Это может произойти намеренно или случайно. В первом случае сотрудник намеренно устраивается на работу в организацию с целью дальнейшего выведывания секретов, во втором непреднамеренное раскрытие происходит в неформальной обстановке. Прямое копирование информации также называется утечкой по прямым каналам.  
 Для защиты данных в компаниях чаще всего задействована одна основная автоматизированная система, поэтому важно учитывать все технические каналы утечки, которые подразумевают варианты кражи данных с использованием физических свойств системы.  
  
 Типы технических каналов утечки информации:  
1) акустический - несанкционированное считывание звука на объекте информационной деятельности, например, прослушивание телефонных разговоров в режиме реального времени или запись разговоров;  
2) акустоэлектрические - значение, используя звуковые волны, после чего информация передается через сеть питания, и на стороне нападающего, преобразуется в доступную для восприятия форму;  
3) оптический канал является разновидностью кражи данных, в которой вредитель принимает фотографии или проводит долгосрочный визуальный осмотр объекта и т. д.;  
4) виброакустический - значение вибрации создается акустическими волнами, при воздействии их на стены, окна и другие архитектурные сооружения;  
5) электромагнитный – показатели индуктивных датчиков из полей информационной системы, в том числе боковое электромагнитное излучение, которое злоумышленник детектирует с помощью специального оборудования и преобразует в понятную форму.  
 Наиболее распространенным и опасным с точки зрения хранения конфиденциальной информации является акустический канал утечки. Известны тысячи случаев, когда конкурент пытался установить устройства прослушки и звукозаписи на другом объекте. С помощью направленных микрофонов вы можете получить доступ к аудиоинформации в помещении на расстоянии до 200 метров от здания. Другими словами, злоумышленнику достаточно сесть в машину в нескольких кварталах от места переговоров, чтобы легко узнать защищаемую информацию.  
 Практически универсальным каналом утечки информации является акустоэлектрический, поскольку его можно использовать на любом уровне электрической сети; злоумышленнику не нужно использовать дополнительные микрофоны или радиопатчи для считывания данных.

Информация собирается без прямого подключения к сети, используется излучение в виде электромагнитных волн. В некоторых случаях в здании компании могут быть установлены усилители-жучки. Во время их работы конкурент легко считывает магнитные волны на расстоянии до 300 метров от источника данных. Защита от воздействия на акустоэлектрический канал обеспечивается так называемым генератором шума, который способен создавать помехи, чтобы вредитель не мог полностью прочитать информацию.  
 Злоумышленник может прослушивать телефонные разговоры в компании. Для реализации этого канала утечки используются высокочастотные устройства наложения. В результате телефонная линия генерирует модулированный сигнал, который перехватывается конкурентом.  
 Оптический канал доступен, если рабочий процесс компании можно визуально контролировать, фотографировать и снимать на видео. Благодаря получению "картинки" этапов работ злоумышленнику не составит труда раскрыть тайну, которую охраняет предприятие. Защита в этом случае обеспечивается обработкой конфиденциальной информации только в закрытых помещениях без окон с сильной звукоизоляцией.  
 Помимо технических каналов, существует также физический способ кражи, который подразумевает захват материального носителя с конфиденциальной информацией.  
 Компаниям, работающим с конфиденциальной информацией любого типа, необходима собственная комплексная система безопасности, которая является препятствием для злоумышленника на всех уровнях обработки данных. Система защиты должна быть создана с учетом всех выявленных каналов утечки. В дальнейшем служба безопасности отвечает за поддержку автоматизированной системы защиты.  
 Факт кражи информации выявляется двумя основными способами. В первом случае сотрудник становится свидетелем инцидента и может рассказать о том, у кого и как была украдена информация. В этом случае вероятность поимки вора всегда выше до того, как он передаст важные данные конкуренту. Важно не допустить, чтобы организация получила убыток, поэтому они всегда стараются выявить инсайдера "по горячим следам".  
 Во втором случае факт кражи становится известен после того, как конкурирующая компания использовала данные в своих собственных целях. По такому сценарию события развиваются в подавляющем большинстве случаев. Факт кражи, о котором владелец информации не знал, произошел из-за использования злоумышленником уязвимых мест в системе безопасности или из-за отсутствия системы безопасности как таковой.  
 Утечка данных в первую очередь является результатом нарушения метода защиты конфиденциальных данных и основной причиной финансовых и “нематериальных” потерь для компании. При выявлении утечки основная задача службы безопасности - как можно скорее начать действия по выявлению злоумышленника.  
 Расследование проводится в рамках закона. Первым шагом является применение организационных мер и закрытие доступа к данным, так как существует риск повторной кражи. Далее вам следует начать разбирательство. На техническом уровне DLP-системы могут предотвращать утечки, автоматически обнаруживая попытку несанкционированной передачи информации за пределы защищенной среды.  
 На втором этапе расследования служба безопасности определяет тип и способ утечки: случайная или запланированная. Как правило, факт потери по неосторожности или непреднамеренной утечки данных легко выявить на этапах анализа отчета DLP-системы, общения с персоналом или после просмотра видеороликов.  
 В результате утечки информации компания может понести серьезные убытки. Ущерб может быть связан с различными причинами: кражей технологии производства продукции, кражей важных документов, разглашением секретной информации и т.д. Поэтому на этапе разработки системы безопасности следует учитывать все возможные каналы утечки, по которым злоумышленник может получить доступ к защищенной информации.  
 Если утечка уже произошла, компания может только попытаться идентифицировать инсайдера - сотрудника, который украл данные или невольно стал соучастником кражи. Кроме того, если данные поступают от конкурентов, следует решить, как обесценить информацию, чтобы предотвратить возможные потери в будущем.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ:

1. Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1 (последняя редакция).
2. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.
3. Девянин П.H. Садердинов A.A., Трайнев B.A. и др. Учебное пособие. Информационная безопасность предприятия. - M., 2006.- 335.