Введение

Мой выбор на разбор данной темы в связи с тем, что данный вопрос является «болезненным» и крайне насущным, так как вся наша жизнь крепко связана с электронными база данных, интернет ресурсами, Программным обеспечением и Программными продуктами имеющими доступ к различным средствам передачи информации(от web-камер до наших мобильных устройств). Попробуем разобраться в данном вопросе более подробно.

Технические каналы утечки информации

Для начала анализа дадим определение:

Технические каналы утечки информации – каналы утечки защищаемых данных, обусловленные техническими характеристиками используемых для передачи информации средств.

К защищаемым данным относятся данные, являющиеся предметом собственности и подлежащие защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Это, как правило, информация ограниченного доступа, содержащая сведения, отнесенные к государственной тайне, а также сведения конфиденциального характера.

Причины утечек данных и возможные ситуации

Среди распространенных причин утечки информации выделяют такие версии:

- Недостаточная охрана чужих данных (организацией или доверенным лицом).
- Неправильное обращение с устройствами, которые хранят информацию (по техническим причинам).
- Все это происходит при сопутствующих условиях, которые допускают возникновение ситуации утечки:
- Некомпетентность сотрудников, которые занимаются защитой данных, их непонимание важности процесса и халатное отношение к информации в целом.

- Использование нелицензионных средств или не прошедших аттестацию программ по защите клиентов и сохранению их конфиденциальности.
- Плохая степень контроля над средствами по охране сведений.
- Постоянная смена сотрудников, которые занимаются защитой персональных данных.

Вина в утечке информации чаще всего возлагается именно на сотрудников фирм и предприятий, а также на их начальство. От любого злоумышленника можно защититься при желании и компетентности работников. Есть факторы, которые не зависят от компаний:

- Катастрофы крупного масштаба.
- Стихийные бедствия.
- Аварии на технических станциях, отказ работы аппаратуры.
- Плохие погодные условия.

Основами для передачи информации любого вида служат системы связи. Самые простые системы состоят из носителя информации и приемника и получателя сведений, а также канала передачи. Любой сигнал можно передать следующими способами:

- световые лучи;
- электромагнитный способ передачи;
- звуковые волнения;
- материалы и вещества.

Главная задача всей цепи устройств – передача информации в определенную точку без искажения. Последовательность оборудования для передачи информации называют системой связи, а ту часть, которая передает информацию, – каналом передачи данных.

Каждый канал передачи информации имеет ряд характеристик:

- Местоположение начала и конца.
- Форма передачи информации.
- Составляющие, или структура канала.
- Скорость, объемы отправки и получения данных.
- Вид канала и способ передачи (как преобразовывается сигнал).
- Пропускная способность цепи.
- Емкость канала.

Эти системы и каналы используются специально для передачи информации. Но бывают случаи, когда канал возникает в другом месте, он не явный и поэтому называется каналом утечки информации. Канал появляется независимо от источника информации и способа ее передачи.

Средства и системы для обнаружения утечки информации

Любой злоумышленник оставляет следы, даже на уровне передачи невидимых сигналов. Техническое устройство изменяет окружающее пространство. Главная цель разведки – добиться того, чтобы устройства, формирующие канал утечки информации, не были обнаружены как можно дольше.

А задача контрразведки заключается в том, чтобы быстро зафиксировать и найти место утечки информации. Сложность этого процесса в том, что неизвестно, какое именно устройство использует злоумышленник. Чтобы выяснить методику получения данных незаконным путем, важно проследить за всеми направлениями и способами получения информации. Нельзя останавливаться на одном методе, требуется проводить контрразведку комплексно.

Способы предотвращения утечки информации

Для эффективной защиты от всех вышеприведенных способов утечки необходима разработка системы мер безопасности, в которую входят две основные группы действий и мероприятий:

- административные и организационные меры;
- технические и программные меры.

И первая и вторая группы мероприятий перед их внедрением требуют обязательного консультирования с профессионалами, особенно если компания имеет намерение получить лицензию на работу с государственной тайной. Применяемые технические средства должны быть сертифицированы и допущены к обороту на территории РФ, недопустимо в целях защиты информации использовать или не опробованные, или запрещенные, относящиеся к категории «шпионских». Защита информации должна основываться только на правовых методах борьбы.

Система безопасности должна проектироваться комплексно, опираясь как на базис на организационные меры. Все ее элементы должны составлять единый комплекс, контроль над работоспособностью которого должен быть возложен на компетентных сотрудников.

Принципы проектирования систем защиты

Существуют определенные принципы, на которых должна основываться комплексная система мер по защите конфиденциальной информации от утечек:

- непрерывность работы системы в пространстве и времени. Используемые способы защиты должны контролировать весь и материальный, и информационный периметр круглосуточно, не допуская возникновения тех или иных разрывов или снижения уровня контроля;
- многозональность защиты. Информация должна ранжироваться по степени значимости, и для ее защиты должны применяться разные по уровню воздействия методы;
- расстановка приоритетов. Не вся информация одинаково важна, поэтому наиболее серьезные меры защиты должны применяться для сведений, имеющих наивысшую ценность;
- интеграция. Все компоненты системы должны взаимодействовать между собой и управляться из единого центра. Если компания холдинговая или имеет несколько филиалов, необходимо настроить управление информационными системами из головной компании;
- дублирование. Все наиболее важные блоки и системы связи должны быть продублированы, чтобы в случае прорыва или уничтожения одного из звеньев защиты ему на смену пришел контрольный.

Построение систем такого уровня не всегда требуется небольшим торговым фирмам, но для крупных компаний, особенно сотрудничающих с государственным заказчиком, оно является насущной необходимостью.

ИБ сопровождение

Так как данный аспект является наиболее выгодным решением проблема с возможной утечкой информации, многие компании, если не сказать, что все, прибегают к помощи агрегаторов ИБ. В нашей стране их широкий спектр. В основном данные компании связаны между собой и имеют схожую структуру ведения ИБ.

Нормативно-правовые акты по ИБ

- федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- ФЗ от 29.11.1994 № 77-ФЗ «Об обязательном экземпляре документов»

- ФЗ РФ от 27.12.1991 № 2124 – 1 «О средствах массовой информации», представляющий собой комплексный нормативный акт, регламентирующий отношения, возникающие в процессе организации и функционирования средств массовой информации (СМИ)»
- ФЗ РФ от 21.07.1993 № 5485 – 1 «О государственной тайне»
- ФЗ от 07.07.2003 № 126-ФЗ «О связи»
- ФЗ от 06.04.2011 № 63-ФЗ «Об электронной подписи»
- ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных»
- ФЗ от 28.07.2012 № 139-ФЗ «О внесении изменений в федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты»

Заключение

В завершении своего анализа и проведенных изучений материалов, хотел бы выделить, что законодательная база и руководства по ведению ИБ имеют правки и ежегодные корректуры. Это указывает на то, что наша страна не стоит на месте в данных вопросах и уделяет пристальное внимание к проблематике утечке и защиты информации.