+++ЗАЩИТА ИНФОРМАЦИИ

Сегодня информацию считают основной ценностью. Ее относят к разряду важнейших ресурсов, сохранность которых является насущной задачей. Чем крупнее организация или сообщество, тем больше усилий прилагается для защиты информации. Попытки хищения или иные варианты враждебного использования сведений предпринимаются часто. Их цели различаются, но последствия всегда отрицательные.

Существует много способов хранения данных – от простых бумажных документов до электронных информационных массивов. Для обеспечения информационной безопасности нужны соответствующие организационные меры и технические средства. В этом направлении разработано множество мероприятий, протоколов защиты. Они реализуются в разных форматах, образуют комплексные системы. Рассмотрим их подробнее.

Возможные угрозы

Независимо от способа хранения, основной угрозой для деловой или конфиденциальной информации является доступ посторонних пользователей.

Базы данных могут существовать в разных формах:

- физические текстовые документы;
- электронные файлы, хранящиеся в памяти компьютеров или на серверах;
- файлы, находящиеся на внешних носителях – жестких дисках, флешках, CD.

Существуют разные виды несанкционированного доступа:

- целенаправленное обращение к базам данных, совершенное с целью их использования;
- случайный доступ, вызванный сбоем систем технической защиты информации.

Оба варианта одинаково недопустимы. В результате таких ситуаций возникает возможность несанкционированного изменения, копирования, тиражирования информационных ресурсов.

Различают несколько источников угроз:

- человеческий фактор;
- сбой компьютерных систем защиты;
- природные катаклизмы, стихийные бедствия, в результате которых штатные средства контроля оказались неэффективными.

Основную проблему представляет антропогенный фактор. В преступных схемах могут быть задействованы как посторонние люди, так и недобросовестные сотрудники организации. Нередко в потере важных сведений оказываются виноваты доверенные лица компании, которые преследовали собственную выгоду. Известно немало примеров подобных действий, когда конфликтные ситуации или корысть побуждают людей использовать данные в собственных целях. Такие угрозы представляют собой наивысшую опасность, отследить враждебные намерения могут не все средства защиты информации. Поэтому, помимо обычных способов контроля и управления деятельностью информационных систем, важно учитывать психологию и мотивацию сотрудников.

Прогнозировать поведение сотрудников умеют DLP! Модуль автоматизированного профайлингга «СёрчИнформ ProfileCenter» составляет психологические портреты работников по анализу их переписки.

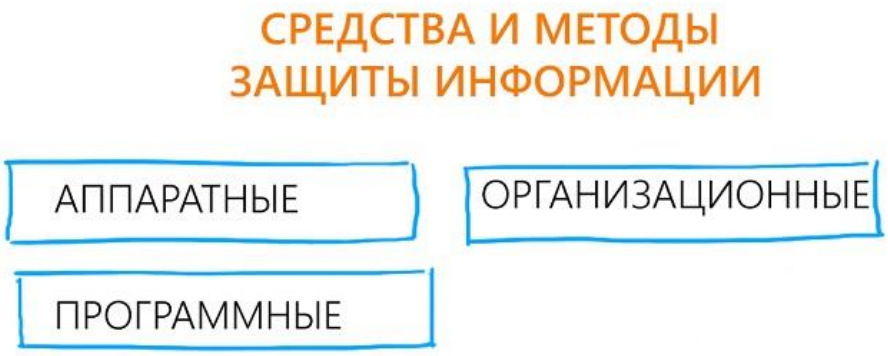
Средства защиты

Средствами защиты информации называют совокупность организационных мер, технических устройств или программных продуктов, которые используются для предотвращения утечки или несанкционированного применения подконтрольных данных.

Средства защиты условно делят на следующие группы:

- **аппаратные, или технические.** Это все приборы или устройства, в том числе технические, механические или электронные, призванные обеспечить контроль доступа к защищенным массивам данных. Кроме этого, аппаратные средства способны маскировать, глушить или шифровать информационные потоки, отказывая в доступе к информации посторонним лицам;

- **программные средства** способны работать только в компьютерной среде. Основными видами являются антивирусы, идентификаторы, приложения для текстового контроля и прочие программы. Максимальная опасность исходит из Сети, поэтому большинство программных средств ориентировано на отсечку несанкционированного внедрения в систему. Кроме этого, используются смешанные аппаратно-программные системы, одновременно выполняющие обе функции;
- **организационные методы защиты** представляют собой технические мероприятия по обеспечению безопасности информации. Сюда входит соблюдение технических норм при подготовке помещений, прокладке кабелей. Кроме этого, к организационным методам относятся нормы правового характера. Это рабочие правила, корпоративные регламенты, законодательные нормы Российской Федерации. Такие методы дают широкий охват всей деятельности организации (или всей отрасли), но в значительной степени зависят от человеческого фактора.



Аппаратные методы преимущественно являются средствами контроля. Они ориентированы на идентификацию личности, шифрование данных и периодическую проверку подлинности адреса при передаче сведений.

К аппаратным средствам относят:

- провода и кабели специальной конструкции;
- комплекты оборудования для защиты периметра охраняемой территории;
- высокочастотные фильтры на линиях связи;
- ультразвуковые излучатели на стеклах окон кабинетов или переговорных комнат;
- специальные экраны для защиты помещений ограниченного доступа и т. д.

Помимо этого, **используются охранные системы**. Они обеспечивают комплексную защиту периметра, включают видеонаблюдение, контроль доступа людей, пожарную охрану объекта.

Программные средства являются наиболее обширной группой, способной обеспечить комплексную защиту информации от внешних воздействий. Они могут отсекать нежелательные действия:

- попытки соединиться с системой через Интернет;
- несанкционированный доступ к чужому ПК;
- возможность использования информации, прошедшей криптографическую обработку.

Организация защиты информационных массивов

Основным органом защиты информации на территории России является Федеральная служба по техническому и экспертному контролю (ФСТЭК). Она обеспечивает решение всех ключевых вопросов информационной безопасности, в число которых входят:

- общие мероприятия по защите данных, составляющих государственную тайну;
- защита от технической разведки иностранных государств;
- контроль технических каналов передачи данных;
- исключение внешних воздействий на хранилища информации, произведенных с враждебными намерениями.

В рамках общего правового поля система защиты информации управляется президентом РФ, которому подчинены региональные и отраслевые структуры власти. Они вырабатывают нормативы и правила защиты информации, определяют приоритетные направления. Таким образом, помимо личного или корпоративного контроля существуют законодательные нормы и государственная поддержка всех мероприятий по охране информационных баз.

В пределах организации процесс охраны данных должен быть продуман так, чтобы не возникало препятствий для работы. Важно принять необходимые меры, но не создавать излишних сложностей. Для этого нужен тщательный анализ источников поступления информации, постоянный контроль каналов передачи и обработки данных. Необходимо определить уровень защиты, распределить нагрузку по техническим, организационным и программным средствам.

В первую очередь понадобится разработка общих правил хранения данных. Полезно рассортировать массивы по степени важности, определив уровень доступа к каждой группе, уточнить порядок пользования сведениями, принять меры, предотвращающие случайную или намеренную утечку сведений в Сеть или на внешние носители. Ограничить вынос текстовых или графических документов, установить ограничение на посещение ненадежных сетевых ресурсов. Такие мероприятия помогут поддерживать корпоративную дисциплину в отношении информации.

«СёрчИнформ Fileauditor» находит в файловой системе документы, которые содержат критичные данные, и ставит на них метки (персональные данные, финансовая информация, договор). Программа отслеживает текущие настройки доступа к файлам и папкам, что облегчает контроль за пользователями в системе.

Для сохранности личной информации важны усилия самого владельца. Не следует раздавать данные кому попало, надеясь на порядочность и аккуратность людей. Пользователи, работающие с чужими данными, несут ответственность согласно действующему законодательству. Однако в процесс всегда могут вмешаться третьи лица. В Сети часто оказываются в свободном доступе базы данных, номера телефонов или другие личные сведения граждан. Это пример беспечного хранения или злонамеренной деятельности мошенников.

Методы и формы защиты

Основным объектом внимания являются компьютеры, работающие отдельно или объединенные в локальную сеть. Особенно уязвимы устройства, имеющие выход в Интернет. Для них необходимы комплексные меры защиты информации, ограничения постороннего доступа и прочие действия, в число которых входят:

- использование антивирусных средств, файрволов;
- меры защиты от случайного и постороннего вмешательства данных от шпионских или диверсионных атак;
- защита информации от электромагнитных воздействий, наводок;
- шифрование данных с целью предотвращения несанкционированного использования.

В состав комплексных методик также входят правовые и организационные меры, действующие в постоянном режиме. В частности, в компаниях используются сложные пароли, созданные для предотвращения постороннего доступа к сведениям.

Все мероприятия разрабатываются на этапе внедрения компьютерных систем. Во время эксплуатации они отрабатываются, способы защиты усиливаются и дополняются по мере появления новых угроз.

К числу наиболее эффективных форм охраны данных относятся:

- общая надежность компьютерных или информационных систем;
- отсечка рискованных или ошибочных операций, исключение доступа неавторизованных пользователей;

• усиление безопасности пользования массивами данных, оптимизация методов передачи или обработки информации;

• резервное копирование сведений;

• профилактические меры безопасности при возникновении аварий, стихийных бедствий.

Важно понимать, что защита информации – не разовая мера, а постоянный и непрерывный процесс. В нем нет второстепенных деталей: любая уязвимость рано или поздно станет каналом утечки данных. Поэтому относиться к мероприятиям по охране сведений надо с максимальной ответственностью и пониманием.

+++СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

Данные в компьютерных системах подвержены риску утраты из-за неисправности или уничтожения оборудования, а также риску хищения. Способы защиты информации включают использование аппаратных средств и устройств, а также внедрение специализированных технических средств и программного обеспечения.

Способы неправомерного доступа к информации

Залогом успешной борьбы с несанкционированным доступом к информации и перехватом данных служит четкое представление о каналах утечки информации.

Интегральные схемы, на которых основана работа компьютеров, создают высокочастотные изменения уровня напряжения и токов. Колебания распространяются по проводам и могут не только трансформироваться в доступную для понимания форму, но и перехватываться специальными устройствами. В компьютер или монитор могут устанавливаться устройства для перехвата информации, которая выводится на монитор или вводится с клавиатуры. Перехват возможен и при передаче информации по внешним каналам связи, например, по телефонной линии.

Методы защиты

На практике используют несколько групп методов защиты, в том числе:

• **препятствие на пути предполагаемого похитителя**, которое создают физическими и программными средствами;

• **управление**, или оказание воздействия на элементы защищаемой системы;

• **маскировка**, или преобразование данных, обычно – криптографическими способами;

• **регламентация**, или разработка нормативно-правовых актов и набора мер, направленных на то, чтобы побудить пользователей, взаимодействующих с базами данных, к должному поведению;

• **принуждение**, или создание таких условий, при которых пользователь будет вынужден соблюдать правила обращения с данными;

• **побуждение**, или создание условий, которые мотивируют пользователей к должному поведению.

Каждый из методов защиты информации реализуется при помощи различных категорий средств. Основные средства – организационные и технические.

Регламент по обеспечению информационной безопасности – внутренний документ организации, который учитывает особенности бизнес-процессов и информационной инфраструктуры, а также архитектуру системы.

Организационные средства защиты информации

Разработка комплекса организационных средств защиты информации должна входить в компетенцию службы безопасности.

Чаще всего специалисты по безопасности:

• **разрабатывают внутреннюю документацию**, которая устанавливает правила работы с компьютерной техникой и конфиденциальной информацией;

• **проводят инструктаж** и периодические проверки персонала; инициируют подписание дополнительных соглашений к трудовым договорам, где указана

ответственность за разглашение или неправомерное использование сведений, ставших известных по работе;

- **разграничивают зоны ответственности**, чтобы исключить ситуации, когда массивы наиболее важных данных находятся в распоряжении одного из сотрудников; организуют работу в общих программах документооборота и следят, чтобы критически важные файлы не хранились вне сетевых дисков;
- **внедряют программные продукты**, которые защищают данные от копирования или уничтожения любым пользователем, в том числе топ-менеджментом организации;
- **составляют планы восстановления системы** на случай выхода из строя по любым причинам.

Если в компании нет выделенной ИБ-службы, выходом станет приглашение специалиста по безопасности на аутсорсинг. Удаленный сотрудник сможет провести аудит ИТ-инфраструктуры компании и дать рекомендации по ее защите от внешних и внутренних угроз. Также аутсорсинг в ИБ предполагает использование специальных программ для защиты корпоративной информации.

Технические средства защиты информации

Группа технических средств защиты информации совмещает аппаратные и программные средства. **Основные**:

- резервное копирование и удаленное хранение наиболее важных массивов данных в компьютерной системе – на регулярной основе;
- дублирование и резервирование всех подсистем сетей, которые имеют значение для сохранности данных;
- создание возможности перераспределять ресурсы сети в случаях нарушения работоспособности отдельных элементов;
- обеспечение возможности использовать резервные системы электропитания;
- обеспечение безопасности от пожара или повреждения оборудования водой;
- установка программного обеспечения, которое обеспечивает защиту баз данных и другой информации от несанкционированного доступа.

В комплекс технических мер входят и меры по обеспечению физической недоступности объектов компьютерных сетей, например, такие практические способы, как оборудование помещения камерами и сигнализацией.

Аутентификация и идентификация

Чтобы исключить неправомерный доступ к информации применяют такие способы, как идентификация и аутентификация.

Идентификация – это механизм присвоения собственного уникального имени или образа пользователю, который взаимодействует с информацией.

Аутентификация – это система способов проверки совпадения пользователя с тем образом, которому разрешен допуск.

Эти средства направлены на то, чтобы предоставить или, наоборот, запретить допуск к данным. Подлинность, как правила, определяется тремя способами: программой, аппаратом, человеком. При этом объектом аутентификации может быть не только человек, но и техническое средство (компьютер, монитор, носители) или данные. Простейший способ защиты – пароль.

+++Как защитить компанию от утечки финансовой и другой секретной информации

Анализируя результаты исследования об утечке финансовой и другой конфиденциальной информации компаний, можно сказать, что почти в половине случаев «секреты фирмы» становятся чужим достоянием совершенно случайно. Мы выяснили слабые места в защите информации от утечек по техническим каналам, а также способы предотвращения инцидентов.

Одной из самых уязвимых в плане утечек является информация, напрямую касающаяся бухгалтерии: финансовая документация, отчетность, бизнес-планы, договоры, цены, зарплата, персональные данные сотрудников.

Как утекает информация

Источников, через которые информация уходит из компании, предостаточно: различные мессенджеры (Skype, ICQ и пр.), электронная почта, открытые источники (социальные сети, форумы), бумага, флешки, диски, резервные копии. Причем и в случае со случайными утечками, и в случае с умышленным сливом источники одни и те же.

Кстати, для получения секретной информации существует чуть ли не целая отрасль – **незаконная и конкурентная разведка**. Первая подразумевает шпионаж: те, кому нужны сведения, вербуют сотрудников компании либо внедряют в штат своего человека. Конкурентная разведка действует открыто – через социальные сети, собеседования, открытые источники информации.

Признаки, которые могут навести на мысль о том, что рядом идет торговля «секретами фирмы»

Во-первых, от компании **уходят клиенты** – вероятнее всего конкурентам кто-то слил клиентскую базу.

Во-вторых, очевидная **перемена в поведении некоторых сотрудников**: внезапное улучшение материального положения, снижение заинтересованности в работе, активизировавшаяся переписка в интернете, частая пересылка графических или запароленных архивированных файлов.

В-третьих, «кучкование». Так, в одной компании 30 из 40 сотрудников, которые занимались заключением договоров, сговорившись, **зарегистрировали собственную организацию** и фактически работали на нее. Сотрудники предлагали клиентам, с которыми напрямую общались, те же услуги, но немного дешевле и перезаключали с ними договоры уже от имени собственной организации.

Действенные способы предотвратить утечку

- **Трудовой договор**. В нем можно прямо прописать, что работодатель имеет полный доступ к информации на компьютерах работников, а в случае разглашения коммерческой тайны будет требовать возмещения убытков. Эти меры являются мощным сдерживающим психологическим фактором.
- **Высокая зарплата**. Боязнь ее потерять скорее всего отобьет у сотрудника желание предавать свою компанию.
- **Слежка и прослушка**. Существуют программы, которые контролируют все, что происходит на компьютере. Если сотрудники знают, что она у них установлена, у них вряд ли появится желание передавать секретную информацию с рабочего компьютера. Еще устанавливают свои «жучки» в кабинетах или переговорках, а «жучки» шпионов блокируют шумогенераторами, которые создают помехи и глушат сигнал.
- **Тренинг**. Устраивают провокацию: сотрудникам рассылают письма с вирусами, просят по телефону выдать конфиденциальные сведения и т. п. В результате теста выясняется, как персонал реагирует на такие действия, и разрабатываются меры защиты.
- **DLP-система (Data Leak Prevention)**. Она отслеживает пересылку и распечатку файлов, внезапные всплески интернет-общения, посещение нехарактерных для работы сайтов и т. д. Также проводит лингвистический анализ переписки и документов и по ключевым словам устанавливает опасность утечки. Работу с DLP-системой важно поручить компетентному специалисту. Если в компании нет ИБ-отдела, настраивать систему и купировать инциденты может сотрудник на аутсорсинге.

Каналы утечки информации

БУМАЖНЫЕ ДОКУМЕНТЫ

С помощью бумаги конфиденциальная информация становится доступной другим чаще всего. Причем независимо от того, сливает ее кто-то умышленно или утечка происходит случайно. Продавать «секреты» на бумаге безопаснее, чем в электронном виде, так как сложно доказать, от кого они получены (если, конечно, нет записи).

КОМПЬЮТЕРЫ

Компьютеры (имеются в виду стационарные) — второй по распространенности канал, через который инсайдеры сливают на сторону конфиденциальную информацию. Но, по сути, компьютер даже больше не канал передачи секретных данных, а канал их получения. Через него инсайдер имеет доступ к корпоративным сведениям, хранящимся на сервере компании, может скачать их на съемные носители или отправить по электронной почте.

ИНТЕРНЕТ

Случайная утечка может произойти, когда финансовые сведения содержатся в программах компании, работающих через интернет, а вход в них имеет примитивные пароли. Таковыми принято считать цифровые или буквенные пароли по ходу клавиатуры: 123456, 123123, 12345678, qwerty, а также abc123, dragon, 111111, iloveyou, sunshine, passw0rd, superman, football и др.

ЭЛЕКТРОННАЯ ПОЧТА

Сотрудники считают, что пересылать секретные данные безопаснее с личной, а не с корпоративной почты. Это заблуждение: установить, чей адрес, легко по учетным записям. Также «электронка» помогает проникнуть в тайны компании с помощью зараженных вирусами писем. Шпионы изучают интересы сотрудника (в соцсетях и т. п.), затем отправляют ему такое письмо, которое он наверняка откроет, допустим коллекционеру плюшевых мишек сообщение с темой «Прикольный мишка».

СМАРТФОНЫ, НОУТБУКИ

Смартфоны и ноутбуки тоже не самый распространенный канал утечки секретной информации, но часто используется менеджерами высшего звена. Ситуация: идет конфиденциальное совещание. У присутствующих с собой смартфоны или, что чаще всего, ноутбуки с материалами совещания. Присутствующий инсайдер активирует встроенный микрофон и сидит себе с невинным видом. А потом все, о чем говорилось на закрытом совещании, сливается во внешний мир.

СЪЕМНЫЕ НОСИТЕЛИ И РЕЗЕРВНЫЕ КОПИИ

Флешки, переносные жесткие диски в силу своего удобства тоже используются для передачи информации. При этом инсайдер может легко сослаться на их обычную потерю. Иногда информация уходит по оплошности. К примеру, сотрудник взял на флешке отчеты с финансовыми показателями домой доработать, а дома незащищенное интернет-соединение. Что касается резервных копий, то хранить в них данные можно в интернете (пример — iCloud).

++ Защита информации, составляющей коммерческую тайну

Коммерческие компании генерируют массивы информации, которая представляет ценность как для самой компании, так и для конкурентов. Критически важные для бизнеса сведения включают входить технологии, ноу-хау, изобретения и разработки, исследования рынка, стратегические планы и другие виды данных, являющиеся самостоятельным активом. Интерес для конкурирующих фирм представляют также сведения о клиентах и контрагентах.

Государство признает информацию активом и вовлекает в гражданско-правовой оборот, устанавливая определенные меры защиты, эквивалентные мерам защиты материальных активов, Специфика методов и инструментов защиты информации, составляющей коммерческую тайну, связана с тем, что данные отражаются в электронном виде и на бумажных носителях.

Определение понятий

Следует различать два неравнозначных понятия. «Коммерческая тайна» и «информация, составляющая коммерческую тайну» одновременно фигурируют в законодательстве, но подразумеваются немного различные явления.

Термин **«коммерческая тайна»** относится к режиму конфиденциальности или к системе защитных организационных мероприятий, которые устанавливаются в компании, чтобы защитить информацию от преступных посягательств или утечек. Режим конфиденциальности помогает компании удержать позиции на рынке, сохранить конкурентные преимущества, избежать расходов на восстановление репутации, пошатнувшейся вследствие разглашения или утечки чувствительных сведений.

«Информация, составляющая коммерческую тайну» – это объем сведений, которые компания определяет произвольно. Сведения могут относится к научной, производственной, маркетинговой деятельности. Реальная или потенциальная коммерческая ценность подобных сведений увеличивается благодаря недоступности для третьих лиц. В отношении сведений устанавливают режим коммерческой тайны.

Массивы информации, составляющей коммерческую тайну, разделяются на четыре группы:

1. **Сведения научно-технического характера**: изобретения, ноу-хау, патенты; рационализаторские предложения; методы повышения эффективности производства; все, что относится к работе компьютерных сетей, стандарты безопасности, программное обеспечение, пароли.
2. **Сведения технологического и производственного характера:** чертежи; модели; документация на оборудование; рецепты производства; методики; описание бизнес-процессов; производственные и маркетинговые планы, стратегии, бизнес-планы; инвестиционные предложения.
3. **Сведения финансового характера**, не являющиеся информацией общего доступа: данные управленческого и финансового учета; отчеты; сведения о себестоимости продукции; расчеты денежного потока; механизмы формирования цен; прогнозируемые налоговые отчисления.
4. **Сведения бизнес-характера**: данные о поставщиках и подрядчиках; информация о клиентах; планы продаж; различные стратегии; консалтинговые рекомендации; данные анализа рынков и аналогичные сведения.

Градация степени конфиденциальности для каждой группы включает:

- высшая степень секретности, доступная только топ-менеджменту организации;
- строго конфиденциальная информация;
- конфиденциальная информация;
- сведения ограниченного доступа.

Ранжирование по уровню конфиденциальности помогает лучше организовать систему доступа и позволяет минимизировать риски утечки. Например, данные наивысшей ценности будут недоступны широкому кругу сотрудников компании, а значит, меньше подвержены риску намеренной или случайной утечки.

Чтобы воспользоваться законными возможностями по защите коммерческой тайны, на первом этапе компания должна определить перечень сведений, на которые распространяется режим коммерческой тайны. И в дальнейшем обоснованно требовать от сотрудников с контрагентами выполнения мер по защите данных и привлекать к ответственности за разглашение информации, составляющей коммерческую тайну.

Параллельно с определением сведений необходимо установить режим конфиденциальности. Это означает – разработать и внедрить систему административно-организационных и технических мер, которые помогут предотвратить умышленное или неумышленное разглашение или распространение сведений.

Правовое регулирование режима коммерческой тайны в сфере гражданского и уголовного законодательства. Правоотношения регулируются Гражданским кодексом, в котором тайна определяется в качестве объекта защиты. Отдельные нормы, касающиеся соблюдения режима коммерческой тайны, содержаться в Трудовом кодексе. Уголовный кодекс вводит ответственность за умышленное разглашение информации. Таким образом, компания вправе самостоятельно определять, какие именно данные являются информацией, составляющей коммерческую тайну, а ее защита гарантируется мерами государственного принуждения.

Угрозы

Прежде чем разрабатывать систему защитных мер, чтобы сохранить конфиденциальность информации, и вводить в компании режим коммерческой тайны, необходимо определить наиболее вероятные угрозы безопасности. Угрозы подразделяются на внутренние и внешние.

Внешние угрозы включают три группы субъектов, которые могут быть заинтересованы в получении сведений, составляющих коммерческую тайну:

- непосредственные конкуренты, которые действуют на тех же рынках, или компании, которые планируют выйти на те же рынки и осуществляют различные сценарии подрыва положения компании;
- субъекты, заинтересованные в переделе долей участия в предприятии, рейдерские группировки, миноритарные акционеры и иные лица, которые могут использовать полученные сведения в борьбе за активы;
- субъекты, которые посягают на активы, принадлежащие компании: недвижимость, земельные участки, акции и доли. Получение данных об активах облегчит процесс.

Внутренние угрозы прежде всего связаны с персоналом компании, включая и топ-менеджеров. Сотрудники с доступом к корпоративным информационным системам могут присвоить сведения, составляющие коммерческую тайну, чтобы продать, использовать в собственных коммерческих проектах или распространить среди неопределенно широкого круга лиц с целью причинить вред компании.

Система защиты должна определить все возможные угрозы и включать механизмы борьбы с конкретными опасностями.

Способы получения информации, составляющей коммерческую тайну

Признание информации коммерческой тайной в большинстве случаев не означает конфиденциальность в строгом смысле слова, потому что доступ к данным есть у сотрудников, разработчиков, клиентов и контрагентов. Сведения, которые во внутренних документах компании классифицируются как тайна, могут оказаться в открытом доступе из-за действий контрагентов. Двоякая суть информации, которая признается конфиденциальной, порождает не только незаконные, но и законные способы получить данные.

НЕЗАКОННЫЕ СПОСОБЫ

- Перехват или организация утечек информации из телекоммуникационных сетей.
- Прямое хищение документов.
- Подкуп сотрудников.

ЗАКОННЫЕ СПОСОБЫ

- Изучение СМИ, официальных источников раскрытия данных, например, сайтов, где публикуется бухгалтерская отчетность, картотеки дел арбитражных судов. Открытые источники позволяют составить достаточно точную картину финансового положения и взаимоотношений компании с контрагентами.
- Работа с сотрудниками конкурирующих компаний, у которых есть широкий круг сведений о деятельности компании-цели и которые отвечают на вопросы, не задумываясь о том, что раскрывают собеседникам информацию, составляющую коммерческую тайну.
- Если компания является открытым акционерным обществом, ее проспект эмиссии содержит большинство из сведений, которые относятся к коммерческой тайне. Кроме того, если консультанты при выпуске не связаны ограничениями по распространению сведений, данные их работы также будут содержать существенный объем информации.
- Интервьюирование сотрудников компании, когда ответы на вопросы, прямо не относящиеся к деятельности, не нарушат режим конфиденциальности, но позволят получить большой объем полезной информации.
- Предложение о работе сотрудникам компании, иногда без намерения действительно нанять человека. фактического предоставления. Прием позволяет получить широкий спектр данных о фактической занятости, круге обязанностей, продукции.
- Изучение самой продукции, а также работы поставщиков сырья и комплектующих.
- Все типы наблюдения за компанией и сотрудниками.

- Переговоры о возможном заключении контракта без намерения фактического заключения. Способ позволяет не только собрать большой объем данных, но и получить возможность изучить процесс производства изнутри. Полученная таким образом информация составляет коммерческую тайну, но предоставляется добровольно.

Борьбу с подобными способами собрать данные осложняет их легитимность. Возможные средства противодействия – инструктаж сотрудников, тщательные проверки потенциальных контрагентов, проведение переговоров вне месторасположения компании.

Меры защиты

Основной мерой защиты информации, составляющей коммерческую тайну, станет установление режима коммерческой тайны. Основные мероприятия носят административно-организационный характер. Например, одним из основополагающих элементов системы является трудовой договор, который предусматривает ответственность сотрудников за нарушение режима конфиденциальности. С учетом того, что внешние угрозы проявляются в форме хищения из компьютерных сетей компании информации, составляющей коммерческую тайну, вместе с административными необходимо внедрять и технические меры, гарантирующие полноту защиты.

Административно-организационные меры

В первую очередь административно-организационные меры нацелены на информирование сотрудников о том, какие сведения относятся к коммерческой тайне, и какие обязанности по неразглашению возлагаются на персонал.

Еще одна цель – убедиться, что компания выполнила все требования закона и проявила предусмотрительность. Это усилит позиции в случае возможного судебного процесса против похитителя коммерческой тайны или заказчика похищения, получившего выгоду от преступного деяния.

Административно-организационные меры включают

- Издание приказа о введении режима коммерческой тайны. В документе определяются основные параметры системы защиты и лица, ответственные за организацию защитных мероприятий.
- Определение перечня сведений, относящихся к коммерческой тайне. Часто авторы документов включают в перечень все сведения, о существовании которых знают. Это неверный путь, так как многие данные общедоступны, например, публикуемая отчетность. В случае судебного разбирательства слишком широкий перечень данных может служить основанием для признания всего списка несоответствующим режиму коммерческой тайны. Более целесообразно ограничить перечень действительно ценной информацией. К конфиденциальным нельзя отнести сведения из учредительных документов, большинство данных о штатном расписании, режиме труда, информацию о соблюдении экологических и пожарных требований.
- Разработка системы локальных нормативных актов, которые обеспечат соблюдение режима конфиденциальности и защиту сведений, составляющих коммерческую тайну. Помимо основного документа – положения «О коммерческой тайне» – могут быть разработаны положения о работе со средствами электронно-вычислительной техники, о порядке предоставления информации контрагентам и государственным органам, порядке копирования документации, типовые договоры с контрагентами, приложения к трудовым договорам и другие.
Положение должно включать разделы, посвященные перечислению сведений, определяемых как коммерческая тайна; порядок внесения изменений в перечень или общие критерии, по которым информация признается коммерческой тайной; перечень рангов и уровней допусков лиц с правом оперировать конфиденциальной информацией; процедуру работы с документами и информационными базами, являющимися носителями информации, составляющей коммерческую тайну; права и обязанности рядовых пользователей и лиц, которым доверили функции по обеспечению режима тайны; порядок хранения, учета и уничтожения различных носителей.
Кроме того, положение должно содержать меры ответственности за несоблюдение

требований. Остальные документы, разработанные в соответствии с положением, не должны ему противоречить. Сотрудники компании должны быть ознакомлены с положением. Законодательство не обязывает привлекать к разработке документа профсоюз или другие представительные органы трудового коллектива, но при необходимости их мнение может быть учтено.

- Определение круга лиц, у которых есть право работать с материалами, где содержатся сведения, составляющие коммерческую тайну, и уровень допуска. На этом этапе организационные меры должны взаимодействовать с техническими, так как уровни допуска реализуются в IT-структуре компании. Для более надежной защиты имеет смысл присваивать уровень допуска не только по степени ценности информации, но и по отраслевому характеру. Уполномоченные лица, которые определяются на уровне приказа исполнительного органа, должны быть уведомлены о том, что доверенная им информация составляет коммерческую тайну, и предупреждены о возможности увольнения и других санкций за ее разглашение.
- Разработка трудовых договоров и договоров с контрагентами, которые содержат норму о защите коммерческой тайны. В договор с работниками обязательно включать пункт, которые предупреждает об ответственности за разглашение конфиденциальных сведений и о праве компании обязать сотрудника компенсировать материального ущерба. Закон позволяет также указать в трудовом договоре срок, начинающийся после расторжения трудового договора, в течение которого работник не вправе разглашать информацию, ставшую известной в связи с выполнением трудовых обязанностей. Обычно срок составляет три года. С перечнем информации сотрудник должен быть ознакомлен под подпись. Наличие личной подписи удостоверяет, что работник полностью осознает ответственность и в случае разглашения сведений готов нести наказание.
- Включение в договоры с контрагентами условия о конфиденциальности в случаях, когда информация, доверенная контрагенту или его сотрудникам в связи с выполнением условий договора, составляет коммерческую тайну. Контрагентами подобного рода могут быть аудиторские, консалтинговые, оценочные и другие компании. Пункт в договоре должен обязывать в полном объеме компенсировать ущерб, причиненный разглашением тайны.
- Функционирование грифов «коммерческая тайна» для защиты конфиденциальной информации и средств идентификации копий документов. Это не защищает документы от копирования в целях передачи информации потенциальным заказчикам, но ограничивает распространение среди широкого круга лиц в открытом доступе.
- Особые режимы пользования телекоммуникационным оборудованием, копировальными устройствами, внешней электронной почтой, интернетом. Допуск сотрудника к ресурсам должен осуществляться на основе заявок с обоснованием необходимости использования. Заявки должны согласовываться на уровне руководства сотрудника и служб безопасности.
- Строгий контроль за использованием учетных записей в сетях только владельцами учетных записей с предупреждением о том, что передача пароля может служить основанием для увольнения из-за «разглашения коммерческой тайны».

Технические меры

Среди технических мер защиты информации, составляющей коммерческую тайну, в первую очередь рассматривают программы, позволяющие полностью защитить информационный периметр от утечек, несанкционированного копирования или передачи данных. К таким средствам относятся DLP-системы и SIEM-системы.

Системы класса DLP настраивают таким образом, чтобы максимально исключить хищение информации внутренними пользователями. Системы класса SIEM выявляют угрозы и идентифицируют различные инциденты информационной безопасности, позволяя осуществлять полный риск-менеджмент и обеспечивать защиту от проникновений через внешний периметр защиты.

К техническим мерам защиты можно отнести все способы кодирования и шифрования данных, установление запрета на копирование, контроль компьютеров сотрудников и мониторинг использования учетных записей.

С настройкой и управлением DLP-системой справится выделенная служба информационной безопасности. Для компаний, в которых ИБ-службы пока нет, есть альтернативное решение – услуга ИБ-аутсорсинга, которая включает установку и обслуживание специального ПО.

Правовые способы защиты коммерческой тайны

Если все утечка произошла и распространения конфиденциальная информация избежать не удалось, возникает необходимость привлечь к ответственности виновника и возместить ущерб. Это возможно только в судебном порядке. В суде также может быть оспорено увольнение по основанию «разглашение коммерческой тайны».

В российской судебной практике немало примеров, когда суд встает на сторону компании. Например, Московский городской суд признал законным увольнение сотрудницы, которая передала по электронной почте данные об объемах поставок. Ее уволили на основании подпункта «в» пункта 6 части 1 статьи 81 Трудового кодекса Российской Федерации – разглашение охраняемой законом тайны. А в другом случае Московский городской суд восстановил нарушителя режима коммерческой тайны на работе, так как компания-ответчик не предоставила трудовой договор с истцом, правила внутреннего трудового распорядка содержали, по мнению суда, нечеткие формулировки, а положение о коммерческой тайне или другие регламентирующие документы и вовсе отсутствовали в компании.

Подобные примеры подчеркивают необходимость внимательно относиться к регламентации вопросов, связанных с установлением режима коммерческой тайны. Тогда компании под силу не только защитить важные коммерческие сведения, но и возместить финансовые потери в случае инцидента, который может привести к оттоку клиентов, потере позиций в конкурентной среде и подрыве репутации.

+++ЗАЩИТА ИНФОРМАЦИИ НА ФЛЕШКЕ

Совместное исследование университетов и Иллинойса и Мичигана показало: 48% людей подключают к компьютеру случайно найденные флешки. Мы перевели основные тезисы и выводы, которые показывают, почему важно учитывать поведение пользователей для защиты информации.

При посещении любой конференции по безопасности, вы неизбежно услышите, как «белые» хакеры хвастаются, что могут взломать систему безопасности любой компании, разбросав флешек с вредоносным кодом на парковке этой компании. Эта история является настолько популярной, что была экранизирована в шестом эпизоде сериала Mr Robot. Невольно на ум приходят мысли – подобная атака на самом деле работает или это просто миф?

Для того, чтобы протестировать данную атаку, исследователи разбросали около 300 флешек на территории Иллинойского Университета в городе Шампейн-Урбана и подсчитали сколько человек подсоединили их к компьютерам. Оказалось, что **пользователи поднимали, подсоединяли и кликали по файлам 48% флешек** разбросанных нами. Причем делали они это быстро: первую флешку подняли менее чем через 6 минут.

Эксперимент

Для проверки того, действительно ли пользователи поднимают флешки, найденные на земле, ученые разбросали пять типов флешек на территории Иллинойского Университета: флешки с наклейкой «экзамены» или «конфиденциально», флешки с прицепленными к ним ключами, флешки с ключами и наклейкой с обратным адресом, а также обычные флешки без каких-либо наклеек.

На каждую флешку записали файлы, соответствующие наклейке на флешке:

- личные файлы для флешек без наклеек, флешек с ключами и флешек с наклейкой с обратным адресом;
- файлы, относящиеся к бизнесу, для на флешек с наклейкой «конфиденциально»;
- файлы с информацией по экзаменам для флешек с надписью «экзамены».

Все файлы на самом деле являлись HTML-файлами со встроенным изображением с нашего сервера. Это позволило исследователям без выполнения какого-либо кода на компьютере пользователя обнаружить, была ли подсоединена флешка и был ли открыт файл. Как только пользователь открывал HTML-файл, появлялся вопрос: не желает ли пользователь принять участие в исследовании, ответив на вопрос, почему он подсоединил флешку, и получить за это подарочную карту. 62 пользователя (около 20%) согласились дать ответ.

«Вброс» зараженных флешек очень эффективен для взлома компьютера

Итак, насколько же эффективно разбрасывать USB-флешки со зловредным кодом с целью взлома компьютеров? Как оказалось, очень эффективно: **48% разбросанных флешек пользователи не только подсоединили к компьютеру, но и открыли по крайней мере один файл** на каждой из них. Удивительно высокая степень результативности доказывает факт, что атаки путем разбрасывания флешек являются реальной угрозой, и подчеркивает необходимость обучения и информирования пользователей об опасности подсоединения непроверенных флешек.

Разбрасывание флешек с вредоносным кодом приносит плоды очень быстро

Кроме того, что многие люди подсоединяют USB-флешки, делают это они очень быстро. 20% подсоединенных флешек были подсоединены в течение первого часа, а 50% флешек – в течение 7 часов, как видно из графика ниже.

Это означает, что промежуток времени на то, чтобы обнаружить атаку, очень мал. В данном случае, первые сообщения о наличии странных флешек на территории университета начали появляться на Reddit примерно через сутки после первой волны, однако это не остановило людей в их стремлении подсоединять подсадные USB-флешки.

Определенное значение имеет то, как выглядит флешка

Флешки с наклейками, вызывающими любопытство, чаще открывают, чем флешки без каких-либо отличительной маркировки. Что удивительно, наибольший результат дает прикрепление физических ключей – альтруистическое поведение является наиболее частой причиной просмотра флешек. Ключи с контактными данными владельца открывали реже всего по причине наличия способа найти владельца. Обратите внимание на то, что разница в частоте открывания НЕ является статистически значимой, кроме того, что флешки с обратным адресом подсоединялись менее часто.

Местоположение для открытия зараженной флешки значения не имеет

Это подтверждает тот факт, что хакеру не нужно проникать на территорию жертвы, чтобы провести атаку эффективно. Размещение флешки на парковке так же эффективно, как и в защищенном конференц-зале.

Каждый уязвим к атакам через случайно найденную флешку

Каждый является уязвимым к атаке через найденную флешку: исследователи не обнаружили разницы между демографическими данными, информированностью о правилах безопасности и образованием пользователей, которые подсоединяли флешки.

Почему в исследовании не наблюдается отрицательной корреляции между образованностью по части информационной безопасности и уязвимостью, думайте сами. Но неизбежно возникает вопрос об эффективности обучения информационной безопасности. Предмет, по всей видимости, стоит изучить тщательнее, чтобы обучение информационной безопасности действительно помогало людям быть более защищенными.

Мотивация пользователей

Мотивация в ответах пользователей: на вопрос почему подсоединили флешку, большинство опрошенных ответили, что сделали это из альтруистических побуждений с целью возврата флешки владельцу (68%). Как видно из диаграммы ниже, только 18% сказали, что ими двигало любопытство.

Мотивация в ответах пользователей не соответствуют тому, какие файлы были открыты. Например, в отношении флешек, с прикрепленными физическими ключами, пользователи чаще кликали по фото с зимнего отпуска, чем по резюме, в котором можно было бы найти контактную информацию владельца. Примечательно, что такое же поведение наблюдалось в отношении флешек с обратным адресом, но не в отношении флешек без маркировки.

Результаты данного исследования показывают, что безопасность USB является реальной проблемой, а разбрасывание USB-флешек – дешевый и практичный инструмент для хакерской атаки.