Научно-технический прогресс превратил информацию в продукт, который можно купить, продать, обменять. Нередко стоимость данных в несколько раз превышает цену всей технической системы, которая хранит и обрабатывает информацию.

Качество коммерческой информации обеспечивает необходимый экономический эффект для компании, поэтому важно охранять критически важные данные от неправомерных действий. Это позволит компании успешно конкурировать на рынке.

Определение информационной безопасности

Информационная безопасность (ИБ) – это состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц. Безопасность данных также подразумевает управление рисками, которые связаны с разглашением информации или влиянием на аппаратные и программные модули защиты.

Безопасность информации, которая обрабатывается в организации, – это комплекс действий, направленных на решение проблемы защиты информационной среды в рамках компании. При этом информация не должна быть ограничена в использовании и динамичном развитии для уполномоченных лиц.

Требования к системе защиты ИБ

Защита информационных ресурсов должна быть:

1. **Постоянной.** Злоумышленник в любой момент может попытаться обойти модули защиты данных, которые его интересуют.
2. **Целевой*.*** Информация должна защищаться в рамках определенной цели, которую ставит организация или собственник данных.
3. **Плановой*.*** Все методы защиты должны соответствовать государственным стандартам, законам и подзаконным актам, которые регулируют вопросы защиты конфиденциальных данных.
4. **Активной*.*** Мероприятия для поддержки работы и совершенствования системы защиты должны проводиться регулярно.
5. **Комплексной*.*** Использование только отдельных модулей защиты или технических средств недопустимо. Необходимо применять все виды защиты в полной мере, иначе разработанная система будет лишена смысла и экономического основания.
6. **Универсальной*.***Средства защиты должны быть выбраны в соответствии с существующими в компании каналами утечки.
7. **Надежной*.***Все приемы защиты должны надежно перекрывать возможные пути к охраняемой информации со стороны злоумышленника, независимо от формы представления данных.

Модель системы безопасности

Информация считается защищенной, если соблюдаются три главных свойства.

Первое – **целостность** – предполагает обеспечение достоверности и корректного отображения охраняемых данных, независимо от того, какие системы безопасности и приемы защиты используются в компании. Обработка данных не должна нарушаться, а пользователи системы, которые работают с защищаемыми файлами, не должны сталкиваться с несанкционированной модификацией или уничтожением ресурсов, сбоями в работе ПО.

Второе – **конфиденциальность** – означает, что доступ к просмотру и редактированию данных предоставляется исключительно авторизованным пользователям системы защиты.

Третье – **доступность** – подразумевает, что все авторизованные пользователи должны иметь доступ к конфиденциальной информации.

Достаточно нарушить одно из свойств защищенной информации, чтобы использование система стало бессмысленным.

Этапы создания и обеспечения системы защиты информации

На практике создание системы защиты информации осуществляется в три этапа.

**На первом этапе** разрабатывается базовая модель системы, которая будет функционировать в компании. Для этого необходимо проанализировать все виды данных, которые циркулируют в фирме и которые нужно защитить от посягательств со стороны третьих лиц. Планом работа на начальном этапе служат 4 вопроса:

1. Какиеисточники информации следует защитить?
2. Какова цельполучения доступа к защищаемой информации?

Целью может быть ознакомление, изменение, модификация или уничтожение данных. Каждое действие является противоправным, если его выполняет злоумышленник. Ознакомление не приводит к разрушению структуры данных, а модификация и уничтожение приводят к частичной или полной потере информации.

1. Что являетсяисточником конфиденциальной информации?

Источники в данном случае это люди и информационные ресурсы: документы, флеш-носители, публикации, продукция, компьютерные системы, средства обеспечения трудовой деятельности.

1. Способы получения доступа, и как защититься от несанкционированных попыток воздействия на систему?

Различают следующие способы получения доступа:

* **Несанкционированный доступ** – незаконное использование данных.
* **Утечка** – неконтролируемое распространение информации за пределы корпоративной сети. Утечка возникает из-за недочетов, слабых сторон технического канала системы безопасности.
* **Разглашение** – следствие воздействия человеческого фактора. Санкционированные пользователи могут разглашать информацию, чтобы передать конкурентам, или по неосторожности.

**Второй этап** включает разработку системы защиты. Это означает реализовать все выбранные способы, средства и направления защиты данных.

Система строится сразу по нескольким направлениям защиты, на нескольких уровнях, которые взаимодействуют друг с другом для обеспечения надежного контроля информации.

**Правовой уровень** обеспечивает соответствие государственным стандартам в сфере защиты информации и включает авторское право, указы, патенты и должностные инструкции. Грамотно выстроенная система защиты не нарушает права пользователей и нормы обработки данных.

**Организационный уровень** позволяет создать регламент работы пользователей с конфиденциальной информацией, подобрать кадры, организовать работу с документацией и физическими носителями данных.

Регламент работы пользователей с конфиденциальной информацией называют правилами разграничения доступа. Правила устанавливаются руководством компании совместно со службой безопасности и поставщиком, который внедряет систему безопасности. Цель – создать условия доступа к информационным ресурсам для каждого пользователя, к примеру, право на чтение, редактирование, передачу конфиденциального документа. Правила разграничения доступа разрабатываются на организационном уровне и внедряются на этапе работ с технической составляющей системы.

**Технический уровень** условно разделяют на физический, аппаратный, программный и математический подуровни.

* физический – создание преград вокруг защищаемого объекта: охранные системы, зашумление, укрепление архитектурных конструкций;
* аппаратный – установка технических средств: специальные компьютеры, системы контроля сотрудников, защиты серверов и корпоративных сетей;
* программный – установка программной оболочки системы защиты, внедрение правила разграничения доступа и тестирование работы;
* математический – внедрение криптографических и стенографических методов защиты данных для безопасной передачи по корпоративной или глобальной сети.

Третий, завершающий этап – это поддержка работоспособности системы, регулярный контроль и управление рисками. Важно, чтобы модуль защиты отличался гибкостью и позволял администратору безопасности быстро совершенствовать систему при обнаружении новых потенциальных угроз.

Виды конфиденциальных данных

Конфиденциальные данные – это информация, доступ к которой ограничен в соответствии с законами государства и нормами, которые компании устанавливаются самостоятельно.

* **Личные** конфиденциальные данные: персональные данные граждан, право на личную жизнь, переписку, сокрытие личности. Исключением является только информация, которая распространяется в СМИ.
* **Служебные** конфиденциальные данные: информация, доступ к которой может ограничить только государство (органы государственной власти).
* **Судебные** конфиденциальные данные: тайна следствия и судопроизводства.
* **Коммерческие** конфиденциальные данные: все виды информации, которая связана с коммерцией (прибылью) и доступ к которой ограничивается законом или предприятием (секретные разработки, технологии производства и т.д.).
* **Профессиональные** конфиденциальные данные: данные, связанные с деятельностью граждан, например, врачебная, нотариальная или адвокатская тайна, разглашение которой преследуется по закону.

Угрозы конфиденциальности информационных ресурсов

**Угроза** – это возможные или действительные попытки завладеть защищаемыми информационными ресурсами. **Источниками угрозы** сохранности конфиденциальных данных являются компании-конкуренты, злоумышленники, органы управления. Цель любой угрозы заключается в том, чтобы повлиять на целостность, полноту и доступность данных.

Угрозы бывают внутренними или внешними. **Внешние угрозы** представляют собой попытки получить доступ к данным извне и сопровождаются взломом серверов, сетей, аккаунтов работников и считыванием информации из технических каналов утечки (акустическое считывание с помощью жучков, камер, наводки на аппаратные средства, получение виброакустической информации из окон и архитектурных конструкций).

**Внутренние угрозы** подразумевают неправомерные действия персонала, рабочего отдела или управления фирмы. В результате пользователь системы, который работает с конфиденциальной информацией, может выдать информацию посторонним. На практике такая угроза встречается чаще остальных. Работник может годами «сливать» конкурентам секретные данные. Это легко реализуется, ведь действия авторизованного пользователя администратор безопасности не квалифицирует как угрозу.

Попытка несанкционированного доступа может происходить несколькими путями:

* **через сотрудников**, которые могут передавать конфиденциальные данные посторонним, забирать физические носители или получать доступ к охраняемой информации через печатные документы;
* **с помощью программного обеспечения** злоумышленники осуществляют атаки, которые направлены на кражу пар «логин-пароль», перехват криптографических ключей для расшифровки данных, несанкционированного копирования информации.
* **с помощью аппаратных компонентов** автоматизированной системы, например, внедрение прослушивающих устройств или применение аппаратных технологий считывания информации на расстоянии (вне контролируемой зоны).

Аппаратная и программная ИБ

Все современные операционные системы оснащены встроенными модулями защиты данных на программном уровне. MAC OS, Windows, Linux, iOS отлично справляются с задачей шифрования данных на диске и в процессе передачи на другие устройства. Однако для создания эффективной работы с конфиденциальной информацией важно использовать дополнительные модули защиты.

Пользовательские ОС не защищают данные в момент передачи по сети, а системы защиты позволяют контролировать информационные потоки, которые циркулируют по корпоративной сети, и хранение данных на северах.

Аппаратно-программный модуль защиты принято разделять на группы, каждая из которых выполняет функцию защиты чувствительной информации:

* **Уровень идентификации** – это комплексная система распознавания пользователей, которая может использовать стандартную или многоуровневую аутентификацию, биометрию (распознавание лица, сканирование отпечатка пальца, запись голоса и прочие приемы).
* **Уровень шифрования** обеспечивает обмен ключами между отправителем и получателем и шифрует/дешифрует все данные системы.

Правовая защита информации

Правовую основу информационной безопасности обеспечивает государство. Защита информации регулируется международными конвенциями, Конституцией, федеральными законами и подзаконными актами.

Государство также определят меру ответственности за нарушение положений законодательства в сфере ИБ. Например, глава 28 «Преступления в сфере компьютерной информации» в Уголовном кодексе Российской Федерации, включает три статьи:

* Статья 272 «Неправомерный доступ к компьютерной информации»;
* Статья 273 «Создание, использование и распространение вредоносных компьютерных программ»;
* Статья 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей».