Методы защиты информации и сведений

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

Правовые аспекты использования информационных технологий и программного обеспечения. Правовое регулирование в области информационной безопасности.

В Концепции национальной безопасности Российской Федерации определены важнейшие задачи в информационной сфере, в том числе и в правовой области:

· установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;

· разработка нормативной правовой базы и координация деятельности федеральных органов государственной власти и других органов, решающих задачи обеспечения информационной безопасности при ведущей роли Федерального агентства правительственной связи и информации при Президенте Российской Федерации.

Законодательство России в области информатизации начало формироваться с 1991 года.

Основополагающим понятием в области правового обеспечения является **информация.**

Закон РФ “Об информации, информатизации и защите информации” определяет понятие **информация**как “сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления”.

При решении организационно-правовых вопросов обеспечения информационной безопасности исходят из того, что информация подпадает под нормы вещного права, что дает возможность применять к информации нормы Уголовного и Гражданского права в полном объеме.

Впервые в правовой практике России информация как объект права была определена в ст. 128, ч. 1, принятого в ноябре 1994 г. ГК РФ,где говориться: “К объектам гражданских прав относятся …информация; результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность)…”. Данная статья дает возможность квалифицировать посягательства на сохранность и целостность информации, как преступления против собственности.

Этим же Законом определено, что **информационные ресурсы,**т. е. отдельные документы или массивы документов, в том числе и в информационных системах, являясь объектами отношений физических, юридических лиц и государства, подлежат обязательному учету и защите как материальное имущество собственника (ст.4.1,ст.6.1.). При этом собственнику предоставляется право самостоятельно в пределах своей компетенции устанавливать режим защиты информационных ресурсов и доступа к ним (ст.6.7).

Законодательные меры

Законодательные меры занимают около 5% объема средств, расходуемых на защиту информации. Это меры по разработке и практическому применению законов, постановлений, инструкций и правил эксплуатации, контроля как аппаратного, так и программного обеспечения компьютерных и информационных систем, включая линии связи, а также все объекты инфраструктуры, обеспечивающие доступ таким системам. В России деятельность в информационной сфере регулируют более 1000 нормативных документов. Уголовное преследование за преступления в этой сфере осуществляется в

соответствии с гл. 28 Уголовного кодекса РФ «Преступления в сфере компьютерной информации», содержащей три статьи.

1. Ст. 272 - несанкционированный доступ к информации. ***Несанкционированный доступ к информации - нарушение установленных правил разграничения доступа с использованием штатных средств, предоставляемых ресурсами вычислительной техники и автоматизированными системами (сетями).***

Отметим, что при решении вопроса о санкционированное доступа к конкретной информации необходимо наличие документа об установлении правил разграничения доступа, если эти правила не прописаны законодательно.

2. Ст. 273 - создание, использование и распространение (включая продажу зараженных носителей) вредоносных программ для ЭВМ, хотя перечень и признаки их законодательно не закреплены. Вредоносная программа -специально созданная или измененная существующая программа, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ или их сети.

3. Ст. 274 - нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Это нарушение работы программ, баз данных, выдача искаженной информации, а также нештатное функционирование аппаратных средств и периферийных устройств; нарушение нормального функционирования сети, прекращение функционирования автоматизированной информационной систем в установленном режиме; сбой в обработке компьютерной информации.

Уголовное преследование за незаконные действия с общедоступной информацией осуществляется в соответствии со ст. 146 «Нарушение авторских и смежных прав» и 147 «Нарушение изобретательских и патентных прав» гл. 19 «Преступления против конституционных прав и свобод человека и гражданина» Уголовного кодекса РФ.

Ответственность за соблюдением сотрудниками организации или компании законодательных мер по защите информации лежит на каждом сотруднике организации или компании, а контроль за их соблюдением - на руководителе.

В существующей практике можно выделить следующие основные аспекты решения проблемы защиты информации:

· анализ правового обеспечения;

· реализация организационно-правовых мероприятий защиты;

· реализация технических мероприятий по защите информации.

Комплексное изучение установленных норм и правил в конкретной прикладной области всегда является обязательным элементом культуры работающего в этой области специалиста.

Анализ правового обеспечения планируемых к осуществлению мероприятий в области организации защиты информации всегда должен предшествовать принятию окончательного решения о реализации этих мероприятий.

К организационно-правовым мероприятиям по защите конфиденциальной информации относятся мероприятия по разработке и принятию определенных документов предприятий и организаций, регламентирующих степень и порядок допуска собственных сотрудников, а также сторонних лиц и организаций к конкретным информационным ресурсам.

Организационно-правовая защита информации реализуется путем установления на предприятии режима конфиденциальности. Можно выделить три формы конфиденциальных отношений:

· Между сотрудником предприятия и самим предприятием как юридическим лицом. Реализуется на практике путем составления соответствующего трудового договора или контракта, заключаемого с сотрудником предприятия.

· Складывающиеся между конкретным сотрудником и другими сотрудниками этого предприятия. Эти отношения развиваются как по вертикали, так и по горизонтали. Указанные отношения называются конфиденциальными отношениями по служебным функциям. Юридически эти отношения закрепляются многообразными административно-правовыми решениями, например приказами о выполнении определенных работ, и регламентируются “Должностными инструкциями”.

· Складывающиеся в рамках хоздоговорных работ и базирующиеся на договоре между партнерами. Юридически конфиденциальные отношения закрепляется в виде четко сформулированных требований и обязательств, которые выдвигают договаривающиеся стороны, и фиксируют в договоре.

В вопросах реализации технических мероприятий обеспечения информационной безопасности с точки зрения правового обеспечения основное внимание следует уделять выполнению требований лицензирования исполнителей работ и использования сертифицированных средств защиты, а также действующим ограничениям на применение специальных технических средств.

Основными проблемы правового обеспечения информационной безопасности являются:

Защита прав на получение информации - предполагает обеспечение условий, препятствующих преднамеренному сокрытию или искажению информации при отсутствии для этого законных оснований. В соответствии со ст.29 Конституции РФ, “Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом”