Содержание:

Введение

С самых давних времен человек занимался обработкой информации, и на протяжении всего времени он изобретал новые способы обработки, стараясь придумать более эффективные методы работы с данными, которые отнимали бы меньше времени, ресурсов и прочих затрат.

Одним из важнейших критериев работы с данными является обеспечение информационной безопасности — сохранения целостности, доступности и конфиденциальности информации, в каком бы виде она не была. Раньше, когда информация хранилась на бумаге, обеспечить ее целостность на долгое время было сложнее, так как бумага со временем портилась, по сравнению с нынешними цифровыми копиями информации, зато конфиденциальность этой информации была более надежной, так как не каждый мог получить доступ к этой информации из любой точки мира, в отличие от документов, которые хранятся в мировой паутине.

Методы защиты информации менялись одновременно со способами ее создания, хранения и обработки, и проблема обеспечения информационной безопасности являлась актуальной во все времена.

В данной курсовой работе объектом исследования будет являться информация. Цель данной курсовой работы — познакомить читателя с основными понятиями, связанными с информационной безопасностью, описать виды защищаемой информации, а также рассказать о методах защиты от информационных угроз.

Глава 1. Основные понятия

Информация — сведения (сообщения, данные) независимо от формы их представления (закон РФ об «Информации, информационных технологиях и защите информации»).

Информационная безопасность — комплекс мер, направленных на обеспечение целостности, доступности и конфиденциальности информации.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

-Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

-Соблюдение конфиденциальности информации ограниченного доступа;

-Реализацию права на доступ к информации.

Целостность информации — способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного или преднамеренного искажения (разрушения).

Доступность информации — состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно.

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Опасности — возможные или реальные явления, события и процессы, способные нанести ущерб или уничтожить индивида, социальную группу, народ, общество, государство и человечество в целом, нанести ущерб благополучию, разрушить материальные, духовные или природные ценности, вызвать деградацию, закрыть путь к развитию науки в целом.

Глава 1.1. Основные виды защищаемой информации

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Перечень сведений, составляющих государственную тайну — совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

- О чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

- О состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

- О привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

- О фактах нарушения прав и свобод человека и гражданина;

- О размерах золотого запаса и государственных валютных резервах Российской Федерации;

- О состоянии здоровья высших должностных лиц Российской Федерации;

- О фактах нарушения законности органами государственной власти и их должностными лицами.

Коммерческая тайна — конфиденциальная информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Информация, составляющая коммерческую тайну — научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введем режим коммерческой тайны.

Банковская тайна — защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также сведения о клиентах и корреспондентах, разглашение которых может нарушить право последних на неприкосновенность к частной жизни.

К основным объектам банковской тайны относятся следующие:

- Тайна банковского счета — сведения о счетах клиентов и корреспондентов и действиях с ними в кредитной организации (о расчетном, текущем, бюджетном, депозитном, валютном, корреспондентском и тому подобных счетах, об открытии, закрытии, переводе, переоформлении счетов и т.д.).

-Тайна операций по банковскому счету — сведения о принятии и зачислении поступающих на счет клиента денежных средств, о выполнении его распоряжений по перечислению и выдаче соответствующих сумм со счета, а также проведении других операций и сделок по банковскому счету, предусмотренных договором банковского счета или законом.

-Тайна банковского вклада — сведения обо всех видах вкладов клиента в кредитной организации.

-Тайна частной жизни клиента или корреспондента - сведения, составляющие личную, семейную тайну и охраняемые законом как персональные данные этого клиента или корреспондента.

Профессиональная тайна — защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

Можно выделить следующие объекты профессиональной тайны:

1. **Врачебная тайна** — информация, содержащая:

- Результаты обследования лица, вступающего в брак;

- Сведения о факте обращения за медицинской помощью, о состоянии здоровья, диагнозе заболевания и иные сведения, полученные при обследовании и лечении

гражданина;

- Сведения о проведенных искусственном оплодотворении и имплантации эмбриона, а также о личности донора;

- Сведения о доноре и реципиенте при трансплантации органов и (или) тканей человека;

- Сведения о наличии психического расстройства, фактах обращения за психиатрической помощью и лечении в учреждении, оказывающем такую помощь, а также иные сведения о состоянии психического здоровья гражданина;

- Иные сведения в медицинских документах гражданина.

2. **Тайна связи** — тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

3. **Нотариальная тайна** — сведения, доверенные нотариусу в связи с совершением нотариальных действий.

4. **Адвокатская тайна** — сведения, сообщенные адвокату гражданином в связи с оказанием ему юридической помощи.

5. **Тайна усыновления** — сведения об усыновлении ребенка, доверенные на законном основании иным лицам, кроме судей, вынесших решение об усыновлении, и должностных лиц, осуществляющих государственную регистрацию этого усыновления.

6. **Тайна страхования** — сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц, полученные страховщиком в результате своей профессиональной деятельности.

7. **Тайна исповеди** — сведения, доверенные гражданином священнослужителю на исповеди.

Служебная тайна — защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в

силу служебной необходимости.

К основным объектам служебной тайны можно отнести такие виды информации, как:

- Служебная информация о деятельности федеральных государственных органов, доступ к которой ограничен федеральным законом в целях защиты государственных интересов;

- Тайна следствия (данные предварительного расследования либо следствия); судебная тайна (тайна совещания судей, содержание дискуссий и результатов голосования закрытого совещания Конституционного суда РФ, материалы закрытого судебного заседания, тайна совещания присяжных заседателей или в силу служебной необходимости, порядок выработки и принятия решения, организация внутренней работы и т.д.);

- Конфиденциальная информация, ставшая известной в силу исполнения служебных обязанностей должностным лицам государственных органов и органов местного самоуправления: коммерческая тайна, банковская тайна, профессиональная тайна, а также конфиденциальная информация о частной жизни лица.

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Обработка персональных данных должна осуществляться на основе принципов:

1. Законности целей и способов обработки персональных данных и добросовестности;

2. Соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

3. Соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

4. Достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

5. Недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

Авторское право распространяется на произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от назначения и достоинства произведения, а также от способа его выражения.

Авторское право распространяется как на обнародованные произведения, так и на необнародованные произведения, существующие в какой-либо объективной форме:

- Письменной (рукопись, машинопись, нотная запись и т.д.);

- Устной (публичное произнесение, публичное исполнение и т.д.);

- Звуко- или видеозаписи (механической, магнитной, цифровой, оптической и т. д.);

- Изображения (рисунок, эскиз, картина, план, чертеж, кино-, теле-, видео- или фотокадр и т. д.);

- Объемно-пространственный (скульптура, модель, макет, сооружение и т. д.);

- В других формах.

Авторское право распространяется на идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты. Авторское право на произведение не связано с правом собственности на материальный объект, в котором произведение выражено.

Объектами авторского права являются:

- Литературные произведения (включая программы для ЭВМ);

- Драматические и музыкально-драматические произведения, сценарные произведения;

- Хореографические произведения и пантомимы;

- Музыкальные произведения с текстом и без текста;

- Аудиовизуальные произведения (кино-, теле- и видеофильмы, слайдфильмы, диафильмы и другие кино- и телепроизведения);

- Произведения живописи, скульптуры, графики, дизайна, графические рассказы, комиксы и другие произведения изобразительного искусства;

- Произведения декоративно-прикладного и сценографического искусства;

- Произведения архитектуры, градостроительства и садово-паркового искусства;

- Фотографические произведения и произведения, полученные способами, аналогичными фотографии;

- Географические, геологические и другие карты, планы, эскизы и пластические произведения, относящиеся к географии, топографии и другим наукам;

- Другие произведения.

Не являются объектами авторского права:

- Официальные документы (законы, судебные решения, иные тексты законодательного, административного и судебного характера), а также их официальные переводы;

- Государственные символы и знаки (флаги, гербы, ордена, денежные знаки и иные государственные символы и знаки);

- Произведения народного творчества;

- Сообщения о событиях и фактах, имеющие информационный характер.

Глава 1.2. Виды и состав угроз информационной безопасности

Угроза безопасности информации — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Фактор, воздействующий на защищаемую информацию — явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение

защищаемой информации, блокирование доступа к ней.

Источник угрозы безопасности информации — субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Уязвимость информационной системы (брешь) — свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Вышеперечисленные угрозы информационным ресурсам реализуются следующими способами:

1. Через имеющиеся агентурные источники в органах государственного управления и коммерческих структурах , имеющих возможность получения конфиденциальной информации (суды, налоговые органы, коммерческие банки и т. д.);

2. Путем подкупа лиц, непосредственно работающих в организации или структурах, напрямую связанных с ее деятельностью;

3. Путем перехвата информации, циркулирующей в средствах и системах связи и вычислительной технике с помощью технических средств разведки и съема информации;

4. Путем прослушивания конфиденциальных переговоров и другими способами несанкционированного доступа к источникам конфиденциальной информации.

С позиции обеспечения безопасности информации в компьютерных системах (КС) все множество потенциальных угроз безопасности информации в КС может быть разделено на два класса.

Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют **случайными или непреднамеренными**.

Стихийные бедствия и аварии чреваты наиболее разрушительными последствиями для информации, так как носители подвергаются физическому разрушению, информация утрачивается или доступ к ней становится невозможен.

Сбои и отказы сложных систем неизбежны. В результате сбоев и отказов нарушается работоспособность технических средств, уничтожаются и искажаются

данные и программы, нарушается алгоритм работы устройств. Нарушения алгоритмов работы отдельных узлов и устройств могут также привести к нарушению конфиденциальности информации.

Ошибки при разработке КС, алгоритмические и программные ошибки приводят к последствиям, аналогичным последствиям сбоев и отказов технических средств. Кроме того, такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы КС. Особую опасность представляют ошибки в ОС и в программных средствах защиты информации.

Ошибки пользователей и обслуживающего персонала — согласно статистике, 65% случаев нарушения безопасности информации происходит благодаря этим ошибкам. Некомпетентное, небрежное и невнимательное выполнение функциональных обязанностей сотрудниками приводят к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты.

Преднамеренно создаваемые угрозы — второй класс угроз безопасности информации, могут быть распределены по пяти группам:

- Традиционный или универсальный шпионаж и диверсии;

- Несанкционированный доступ к информации;

- Электромагнитные излучения и наводки;

- Модификация структур;

- Вредоносные программы.

Средства шпионажа по-прежнему актуальны в качестве методов несанкционированного добывания и уничтожения информации. Они также эффективны и в условиях применения компьютерных систем.

По отношению к отдельной организации существуют следующие виды **внешних угроз**:

- Недобросовестные конкуренты;

- Криминальные группы и формирования;

- Противозаконные действия отдельных лиц и организаций административного аппарата, в том числе и налоговых служб;

- Нарушение установленного регламента сбора, обработки и передачи информации.

Основные виды **внутренних угроз**:

- Преднамеренные преступные действия собственного персонала организации;

- Непреднамеренные действия и ошибки сотрудников;

- Отказ оборудования и технических средств;

- Сбои программного обеспечения средств обработки информации.

Объектами различных угроз в коммерческой деятельности являются:

- Человеческие ресурсы (персонал, сотрудники, компаньоны и др.), включая трудовые и кадровые ресурсы;

- Материальные ресурсы;

- Финансовые ресурсы;

- Временные ресурсы;

- Информационные ресурсы, включая интеллектуальные ресурсы (патенты, ноу-хау, программные продукты и т. д.).

Наиболее опасным источником угроз предприятия выступают собственные сотрудники. Мотивами в этом случае являются безответственность, некомпетентность (низкая квалификация), личные побуждения (самоутверждение, корыстные интересы).

Оценка возможных **потерь** предполагает знание видов потерь и умение вычислять вероятность их возникновение. Существуют следующие виды потерь:

- Материальные — непредусмотренные проектом дополнительные затраты или прямые потери оборудования, сырья, энергии и т. д.;

- Трудовые — потери рабочего времени, вызванные непредвиденными обстоятельствами; измеряется в часах рабочего времени;

- Кадровые — потери профессиональных работников, необходимых предприятию;

- Финансовые — прямой денежный ущерб, связанный с непредусмотренными платежами, штрафами, выплатой налогов, а также потерей денежных средств и ценных бумаг;

- Временные — происходят, когда процесс идет медленнее намеченного срока. Оценка осуществляется в часах, днях, неделях, месяцах запаздывания в получении запланированного результата;

- Информационные потери — одни из самых серьезных потерь в бизнесе, способные привести к краху всей организации;

- Особые виды потерь проявляются в нанесении ущерба здоровью и жизни людей, окружающей среде, престижу предпринимателя, а также вследствие других неблагоприятных социальных и морально-психологических последствий.

Одной из самых серьезных угроз коммерческой деятельности является промышленный шпионаж. Его сущность состоит в стремлении к овладению конфиденциальной информацией конкурентов с целью получения максимальной коммерческой выгоды. Ведется различными средствами, включая использование особых технических средств и подкуп должностных лиц.

Основными каналами утечки информации являются:

- Открытые источники;

- Субъекты-носители информации;

- Технические средства разведки.

К **открытым источникам** относятся каналы, по которым информацию можно почерпнуть без нарушения каких-либо ограничений или запретов — из книг, газет, научных и технических изданий и особенно из рекламных каталогов и брошюр.

Использование субъектов — наиболее распространенный метод промышленного шпионажа. При определенных условиях люди способны воровать, скрывать, продавать информацию и совершать прочие криминальные действия.

Технические средства применяются в случае невозможности использования агентурных средств.

Глава 2. Методы защиты информации

С учетом устоявшейся практики обеспечения информационной безопасности выделяют следующие виды защиты информации:

- Правовая защита информации — защита информации правовыми методами, включая в себя разработку законодательных и нормативных документов, а также надзор и контроль за их исполнением;

- Техническая защита информации — заключается в обеспечении безопасности информации некриптографическими методами безопасности с применением технических, программных и программно-технических средств;

- Криптографическая защита информации — защита информации с помощью средств криптографии (методом шифрования);

- Физическая защита информации — защита путем организации мероприятий и совокупности средств, создающих препятствия для доступа неуполномоченных физических лиц к объекту защиты;

- Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты. При этом к объектам защиты могут быть отнесены охраняемая территория, здание, помещение, информация и/или информационные ресурсы объекта информатизации.

Организационная защита информации — это регламентация деятельности предприятия и взаимоотношений персонала на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Только комплексное применение всех видов защиты информации обеспечивает необходимый и достаточный уровень информационной безопасности предприятия.

Глава 2.1. Правовые основы защиты информации

Правовая защита информации — защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Основные функции правовой базы:

- Разработка основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации;

- Определение системы органов и должностных лиц, ответственных за обеспечение информационной безопасности в стране и порядка регулирования деятельности предприятий и организации в этой области;

- Создание полного комплекса нормативно-правовых руководящих и методических материалов (документов), регламентирующих вопросы обеспечения информационной безопасности как в стране в целом, так и на конкретном объекте;

- Определение мер ответственности за нарушение правил защиты;

- Определение порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации.

В настоящее время основополагающее значение в области информационного права имеют следующие законодательные акты:

- Гражданский кодекс Российской Федерации.

- Кодекс Российской Федерации об административных правонарушениях.

- Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895.

- Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и защите информации»;

- Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»

- Федеральный закон № 17-ФЗ от 3 февраля 1996 г. «О банках и банковской деятельности»;

- Федеральный закон № 63-ФЗ от 6 апреля 2011 г. «Об электронной подписи»;

- Федеральный закон № 152-ФЗ от 27 июля 2006 г. «О персональных данных»;

- Федеральный закон № 98-ФЗ от 29 июля 2004 г. «О коммерческой тайне»;

- Федеральный закон № 126-ФЗ от 7 июля 2003 г. «О связи»;

- Федеральный закон № 77-ФЗ от 29 декабря 1994 г. «Об обязательном экземпляре документов»;

- Федеральный закон № 125-ФЗ от 1 октября 2004 г. «Об архивном деле в Российской Федерации»;

- Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»;

- Закон РФ № 2124-1 от 27 декабря 1991 г. «О средствах массовой информации»;

- Закон РФ № 5485-1 от 21 июля 1993 г. «О государственной тайне»;

- Закон РФ № 2124-1 от 27 декабря 1991 г. «О средствах массовой информации»;

- Закон РФ № 5485-1 от 21 июля 1993 г. «О государственной тайне»;

- Закон РФ №176-ФЗ от 24 июня 1999 г. «О почтовой связи»;

- Закон РФ от 11.03.92 г. № 2487-1 «О частной детективной и охранной деятельности».

Глава 2.2. Техническая защита информации

Техническая защита информации — защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Техника защиты информации — средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Технические средства применяются для решения следующих задач:

- Проведение специальных исследований технических средств обеспечения производственной деятельности на наличие возможных каналов утечки информации;

- Выявление каналов утечки информации на разных объектах и в помещениях;

- Локализация каналов утечки информации;

- Поиск и обнаружение средств промышленного шпионажа;

- Противодействие несанкционированному доступу к источникам конфиденциальной информации и другим действиям.

По функциональному назначению технические средства могут быть классифицированы на средства обнаружения, средства поиска и детальных измерений, средства активного и пассивного противодействия.

По своим техническим возможностям средства защиты информации могут быть общего назначения, рассчитанные на использование непрофессионалами с целью получения предварительных (общих) оценок, и профессиональные комплексы, позволяющие проводить тщательный поиск, обнаружение и прецизионные измерения всех характеристик средств промышленного шпионажа.

В качестве примера первых можно рассмотреть группу индикаторов электромагнитных излучений типа ИП, обладающих широким спектром принимаемых сигналов и довольно низкой чувствительностью. В качестве второго примера - комплекс для обнаружения радиозакладных устройств, предназначенный для автоматического обнаружения и определения местонахождения радиопередатчиков, радиомикрофонов, телефонных закладок и сетевых радиопередатчиков.

Поисковую аппаратуру можно подразделить на аппаратуру поиска средств съема информации и исследования каналов ее утечки.

Аппаратура первого типа направлена на поиск и локализацию уже внедренных зло умышленниками средств несанкционированного доступа. Аппаратура второго типа предназначается для выявления каналов утечки информации.

Обработка результатов измерений осуществляется на ПЭВМ в соответствии с действующими нормативно-методическими документами ФСТЭК России.

Глава 2.3. Программная защита информации

Программная защита информации — это система специальных программ, реализующих функции защиты информации. Выделяются следующие направления использования программ для обеспечения безопасности конфиденциальной информации:

- Защита информации от несанкционированного доступа;

- Защита информации и программ от копирования;

- Защита информации и программ от разрушения и модификации;

- Программная защита каналов связи.

Основные функции программных средств защиты информации:

- Идентификация субъектов и объектов;

- Разграничение доступа у вычислительным ресурсам и информации;

- Контроль и регистрация действий с информацией и программами.

Процедура идентификации и подтверждения подлинности предполагает проверку, является ли субъект, осуществляющий доступ, тем, за кого он себя выдает. Наиболее распространенный метод — идентификация по паролю.

После выполнения процедур идентификации и установления подлинности пользователь получает доступ к вычислительной системе, и защита информации осуществляется на трех уровнях: аппаратуры, ПО и данных.

Средства защиты от копирования предотвращают использование нелегальных копий программного обеспечения и являются единственным средством, защищающим авторские права разработчиков. Под средствами защиты от

копирования понимаются средства, обеспечивающие выполнение программой своих функций только при наличии некоторого уникального некопируемого элемента. Он может быть как техническим (флешка), так и в виде информации (ключ).

Одной из задач обеспечения безопасности является **защита информации от разрушения и модификации.**

Программные средства защиты имеют следующие разновидности специальных программ:

- Идентификации технических средств, файлов и аутентификации пользователей;

- Регистрации и контроля работы технических средств и пользователей;

- Обслуживания режимов обработки информации ограниченного пользования;

- Защиты операционных средств ЭВМ и прикладных программ пользователей;

- Уничтожения информации в защитные устройства после их использования;

- Сигнализирующих нарушения использования ресурсов;

- Вспомогательных программ различного назначения.

Глава 2.4. Программно-техническая защита информации

Программно-технические средства защиты информации направлены на контроль оборудования, программ и/или данных. Центральным для программно-технического уровня является понятие **сервиса безопасности**. В их число входят:

- Идентификация и аутентификация;

- Управление доступом;

- Протоколирование и аудит;

- Контроль целостности;

- Экранирование;

- Анализ защищенности;

- Обеспечение отказоустойчивости;

- Обеспечение безопасного восстановления;

- Туннелирование;

- Управление.

К программно-техническим средствам относят:

Программно-технические средства защиты информации от несанкционированного копирования, в том числе:

- Средства защиты носителей данных;

- Средства предотвращения копирования программного обеспечения, установленного на вычислительную систему.

Программно-технические средства криптографической и стенографической защиты информации (включая средства маскирования информации) при ее хранении на носителях данных и при передаче по каналам связи.

Программно-технические средства прерывания работы программы пользователя при нарушении им правил доступа, в том числе:

- Принудительное завершение работы программы;

- Блокировка компьютера.

Программно-технические средства стирания данных, в том числе:

- Стирание остаточной информации, возникающей в процессе обработки данных в оперативной памяти и на магнитных носителях;

- Надежное стирание устаревшей информации с магнитных носителей.

Программно-технические средства выдачи сигнала тревоги при попытке несанкционированного доступа к информации, в том числе:

- Средства регистрации некорректных обращений пользователей к защищаемой информации;

- Средства организации контроля за действиями пользователей ПК;

- Программно-технические средства обнаружения и локализации действия программных и программно-технических закладок.

Глава 2.5. Физическая защита информации

Физическая защита информации — защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Физические средства защиты — это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.

К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.

Эти средства применяются для решения следующих задач:

- Охрана территории предприятия и наблюдение за ней;

- Охрана зданий, внутренних помещений и контроль за ними;

- Охрана оборудования, продукции, финансов и информации;

- Осуществление контролируемого доступа в здания и помещения.

Все физические средства, на которых строятся системы ограждения и физической изоляции, можно разделить на:

- Средства предупреждения угроз;

- Средства обнаружение угроз;

- Средства ликвидации угроз.

К средствам предупреждения относятся:

- Естественные и искусственные барьеры;

- Особые конструкции периметров, проходов, оконных и дверных переплетов, помещений, сейфов, хранилищ;

- Зоны безопасности.

Естественные и искусственные барьеры служат для противодействия незаконному проникновению на территорию объекта.

Одним из главных физических средств защиты проходов, помещений, сейфов и хранилищ являются **замки**. Они бывают простыми (с ключами), кодовыми (в том числе и с временной задержкой на открывание) и с программными устройствами, открывающие двери и сейфы только в определенные часы.

Важнейшим средством физической защиты является планировка объекта, его зданий и помещений по **зонам безопасности**, которые учитывают степень важности различных частей объекта с точки зрения нанесения ущерба от различного вида угроз. Оптимальное расположение зон безопасности и размещение в них эффективных технических средств обнаружения, отражения и ликвидации последствий противоправных действий составляет основу концепции инженерно-технической защиты объекта.

Зоны безопасности должны располагаться на объекте последовательно, создавая цепь чередующихся друг за другом препятствий (рубежей), которые придется преодолевать злоумышленнику.

К средствам обнаружения угроз можно отнести:

- охранные системы и средства охранной сигнализации;

- охранное телевидение;

-охранное освещение.

Охранные системы и средства охранной сигнализации предназначены для обнаружения различных видов угроз: попыток проникновения на объект защиты, в охраняемые зоны и помещения, попыток проноса (выноса) оружия, средств промышленного шпионажа, краж материальных и финансовых ценностей и других действий, оповещения сотрудников охраны или персонала объекта о появлении

угроз и необходимости усиления контроля доступа на объект, территорию, в здания и помещения.

Эффективность работы системы охраны и охранной сигнализации в основном определяется параметрами и принципом работы датчиков. Применяются датчики следующих типов: механические выключатели, проволока с выключателем, магнитный выключатель, ртутный выключатель, коврики давления, металлическая фольга, проволочная сетка, шифроволновый датчик, ультразвуковой датчик, инфракрасный датчик, фотоэлектрический датчик, акустический датчик, вибрационный датчик, индуктивный датчик, емкостный датчик и другие.

Важным объектом охранной системы является **система тревожного оповещения**: звонки, сирены, подающие постоянные или прерываемые сигналы о появлении угрозы.

Одним из распространенных средств охраны является **охранное телевидение.** Особенностью охранного телевидения является возможность не только отметить нарушение режима охраны предприятия, но и контролировать обстановку вокруг него в динамике ее развития, определять опасность действий, вести скрытое наблюдение и производить видеозапись для последующего анализа правонарушения как с целью анализа, так и для привлечения к ответственности нарушителя.

Источниками изображения (датчиками) в системах охранного телевидения являются видеокамеры. Видеокамера является наиболее важным элементом системы охранного телевидения, так как от ее характеристик зависит эффективность и результативность всей системы контроля и наблюдения. К средствам ликвидации угроз можно отнести **систему пожаротушения**.

Контроль доступа в помещения или здания осуществляется посредством опознавания службой охраны или техническими средствами. Контролируемый доступ предполагает ограничение круга лиц, допускаемых в определенные защищаемые зоны, здания, помещения, и контроль за передвижением этих лиц внутри них. Основанием допуска служит определенный метод опознавания и сравнения с разрешительными параметрами системы. Имеется весьма широкий спектр методов опознавания уполномоченных лиц на право их доступа в помещения, здания, зоны.

На основе опознавания принимается решение о допуске лиц, имеющих на это право, или запрещение — для не имеющих его. Наибольшее распространение

получили **атрибутные и персональные методы** опознавания.

К **атрибутным** способам относятся средства подтверждения полномочий, такие, в частности, как документы (паспорт, удостоверение), карты (фотокарточки, карты с магнитными, электрическими, механическими идентификаторами и т. д.) и иные средства (ключи, сигнальные элементы и т. д.)

Персональные методы — это методы определения лица по его независимым показателям: отпечаткам пальцев, геометрии рук, особенностям глаз. Персональные характеристики бывают статические и динамические. К последним относятся пульс, давление, кардиограммы, речь, почерк и другие.

Системы опознавания по отпечаткам пальцев. В основу идентификации положено сравнение относительного положения окончаний и разветвлений линий отпечатка. Поисковая система ищет на текущем изображении контрольные элементы, определенные при исследовании эталонного образца. Для идентификации одного человека считается достаточным определение координат 12 точек.

Системы распознавания по голосу. Существует несколько способов выделения характерных признаков речи человека: анализ кратковременных сегментов, контрольный анализ, выделение статистических характеристик. Следует отметить, что теоретически вопросы идентификации по голосу разработаны достаточно полно, но промышленное производство пока налажено слабо.

Системы опознавания по почерку считаются наиболее удобными для пользователя. Основным принципом идентификации по почерку является постоянство подписи каждого индивидуума, хотя абсолютного совпадения не бывает.

Все устройства идентификации человека могут работать как отдельно, так и комплексе. Комплекс может быть узкоспециальным или многоцелевым, при котором система выполняет функции охраны, контроля, регистрации и сигнализации.

Запирающие устройства и специальные шкафы занимают особое место в системах ограничения доступа, поскольку содержат в себе признаки как систем физической защиты, так и устройств контроля доступа. Они отличаются большим разнообразием и предназначены для защиты документов, материалов, магнитных и фотоносителей и даже технических средств.

Глава 2.6. Криптографическая защита информации

Криптографическая защита информации — защита информации с помощью ее криптографического преобразования. К средствам криптографической защиты информации относятся аппарпатные, программно-аппаратные и программные средства, реализующие криптографические алгоритмы преобразования информации с целью:

- защиты информации при ее обработке, хранении и передаче;

- обеспечения достоверности и целостности информации (в том числе с использованием алгоритмов цифровой подписи) при ее обработке, хранении и передаче;

- выработки информации, используемой для идентификации и аутентификации субъектов, пользователей и устройств;

- выработки информации, используемой для защиты аутентифицирующих элементов защищаемой АС при их выработке, хранении, обработке и передаче.

Криптографические методы предусматривают **шифрование и кодирование информации.** Различают два основных метода шифрования: симметричный и ассиметричный. В первом из них один и тот же ключ (хранящийся в секрете) используется и для шифрования, и для расшифровывания данных. Существует национальный стандарт на подобные методы — ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

В ассиметричных методах используются два ключа. Один из них, несекретный (может публиковаться вместе с другими открытыми сведениями о пользователе), применяется для шифрования, другой, секретный — для расшифровывания. Самым популярным из ассиметричных является метод RSA, основанный на операциях с большими (100-значными) простыми числами и их произведениями.

Криптографические методы позволяют надежно контролировать целостность как отдельных порций данных, так и их наборов (таких, как поток сообщений), определять подлинность источника данных, гарантировать невозможность

отказаться от совершенных действий (неотказуемость).

В основе криптографического контроля целостности лежат два понятия:

- хэш-функция;

- электронная подпись (ЭП).

Хэш-функция — это труднообратимое преобразование данных (односторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции.

Глава 2.7. Организационная защита информации

Организационная защита информации — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Организация охраны и режима подразумевает комплекс мероприятий по исключению возможности тайного проникновения на территорию в помещение посторонних лиц, создание отдельных охраняемых зон, временного и пропускного режима и организации контроля за персоналом и посетителями.

Организация работы с кадрами подразумевает подбор и расстановку сотрудников на штатные должности, изучение морально-деловых качеств, обучение их правилам работы с конфиденциальной информацией, доведение мер ответственности, контроль за работой персонала.

Работа с документами подразумевает организацию разработки и использования носителей информации, их учета, использования, хранения и уничтожения.

Анализ внутренних и внешних угроз подразумевает выявление, классификацию и постоянное изучение ситуаций, способствующих образованию каналов несанкционированного доступа к конфиденциальной информации в единстве с изучением характера возможных угроз безопасности информации.

Комплексное управление системой защиты подразумевает оптимальное планирование применения всего комплекса средств защиты информации,

технических и физических средств, организацию их эксплуатации и обслуживания.

Сложность обеспечения защиты информации требует создания специальной службы, осуществляющей реализацию всех защитных мероприятий и в первую очередь организационного плана.

Структура, численность и состав подразделения (службы) по защите информации на предприятии определяются реальными потребностями (степенью влияния угроз безопасности информации на показатели работы). Комплексная безопасность предприятия и защита информации может быть реализована следующими тремя путями:

- абонементное обслуживание силами специальных организаций;

- создание собственного подразделения;

- комбинированный вариант.

В первом случае специализированное предприятие (организация), имеющее лицензию на соответствующие виды деятельности, на высоком профессиональном уровне проводит полный комплекс работ, связанный с организацией защиты и поддержание состояния защищенности на должном уровне. Поскольку для получения лицензии для подобного рода деятельности требуются квалифицированные кадры, дорогостоящие аппаратные, программные и технические средства контроля, методики проведения работ, то лицензия - гарантия качества защиты. При этом услуги такого рода достаточно дороги и специалисты не могут постоянно находиться на объекте.

Для решения задач защиты информации на подобное подразделение могут быть возложены следующие функции:

- организовывать и обеспечивать пропускной и внутриобъектовый (при наличии зон ограниченного доступа) режим в зданиях и помещениях, устанавливать порядок несения службы охраны, контролировать соблюдение требований режима сотрудниками, смежниками, партнерами и посетителями;

- руководить работами по правовому и организационному регулированию отношений по защите коммерческой тайны;

- участвовать в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты коммерческой тайны, в

частности Устава, Коллективного договора, Правил внутреннего трудового распорядка, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;

- разрабатывать и осуществлять совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ, организовывать и контролировать выполнение требований «Инструкции по защите коммерческой тайны», «Политики информационной безопасности»;

- изучать все стороны производственной, коммерческой, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, вести учет и анализ нарушений режима безопасности, накапливать и анализировать данные о злоумышленных устремлениях конкурентов и других организаций получить доступ к информации о деятельности предприятия или его клиентов, партнеров, смежников;

- организовывать эксплуатацию систем безопасности, средств защиты информации, поддерживать их в работоспособном и актуальном состоянии;

- организовывать и проводить служебные расследования по фактам разглашения сведений, утрат документов и других нарушений режима безопасности предприятия;

- разрабатывать, вести, обновлять и пополнять «Перечень сведений, составляющих коммерческую тайну» и другие нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;

- обеспечивать строгое выполнение требований нормативных документов по защите коммерческой тайны;

- организовывать и регулярно проводить обучение сотрудников предприятия и службы безопасности по всем направлениям защиты коммерческой тайны;

- вести учет носителей информации, сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;

- вести учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;

- поддерживать контакты с правоохранительными органами по вопросам обеспечения безопасности предприятия и, при необходимости – при проведении служебных проверок по фактам утраты информации.

Для предприятий, в которых создание подобных подразделений является экономически нецелесообразным данные виды работ выполняются либо руководителем предприятия, либо специально назначенным сотрудником.

Заключение

В данной курсовой работе я выполнил поставленные во введении задачи - познакомил читателя с основными понятиями, связанными с информацией и информационной безопасностью, описал виды защищаемой информации, а так же перечислил и раскрыл различные методы защиты информации. Я постарался наиболее полно раскрыть данную мне тему, подробно и доступно объяснив понятия, содержащиеся в данной теме.

Список использованной литературы

www.wikipedia.ru

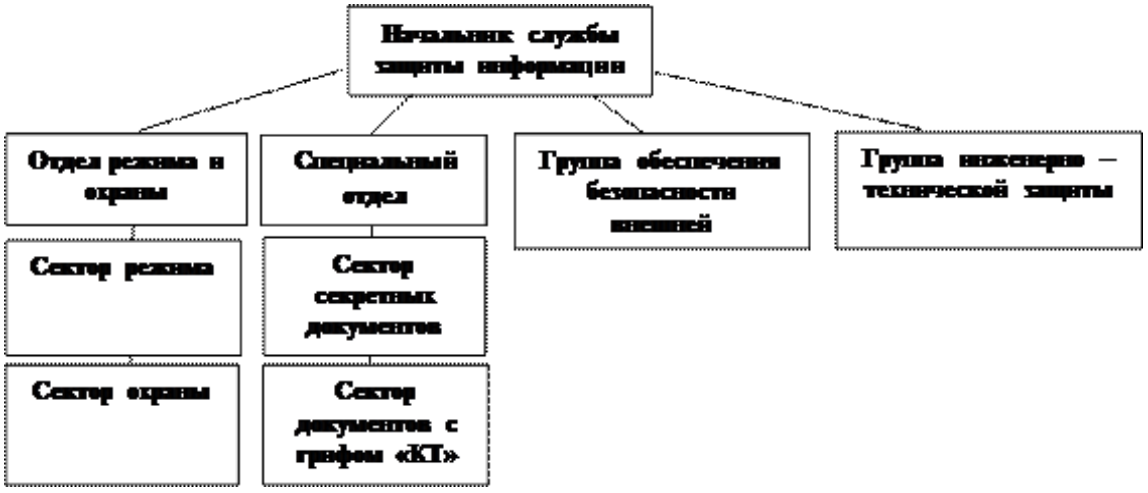
www.studopedia.ru

www.yandex.ru

www.e-biblio.ru

Приложения

Структура подразделения для защиты информации.



Направления организационной защиты информации.

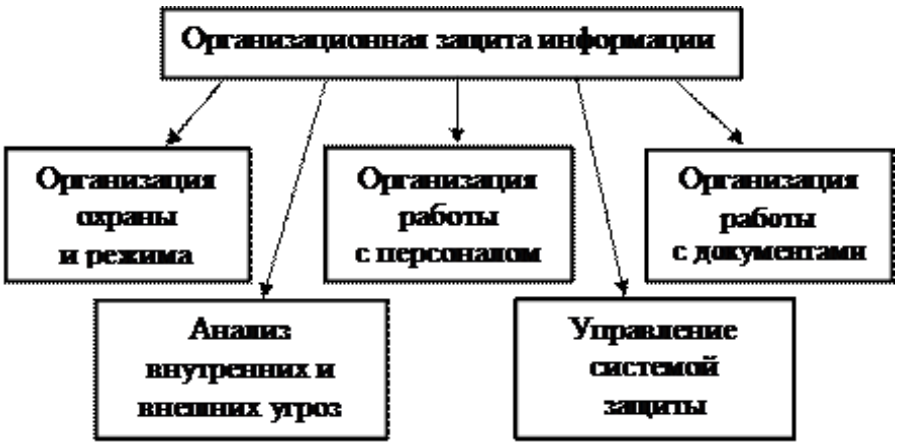


Рис. 5 . Направления организационной защиты информации