Содержание:

Введение

Современное общество называется информационным. Широкое развитие средств вычислительной техники и связи позволило собирать, хранить, обрабатывать и передавать информацию в таких объемах и с такой оперативностью, которые были немыслимы раньше.

Современный этап информатизации связан с использованием персональной электронно-вычислительной техники, систем телекоммуникаций, создания сетей ЭВМ. Однако занимаясь производством технических и программных средств, информационных технологий для получения новых знаний. Формирование информационного общества опирается на новейшие информационные, телекоммуникационные технологии и технологии связи. Именно новые технологии привели к бурному распространению глобальных информационных сетей, открывающих принципиально новые возможности международного информационного обмена.

С развитием информационных технологий и всеобщей компьютеризации привело к тому, что информационная безопасность стала обязательной. И одна из характеристик это информационные системы.

Безопасность информационных систем защищена от случайного или преднамеренного вмешательства в нормальный процесс её функционирования, от попыток хищения (несанкционированного получения) информации.

Угрозой информационной безопасности представляет собой события или действия, которые могут привести к искажению, несанкционированному использованию или к разрушению информационных ресурсов, а также программных и аппаратных средств.

Человек, пытающийся нарушить информационную систему или получить несанкционированный доступ к информации, обычно называется взломщиком, а иногда хакером.

Свои противоправные действия, направленные на обладание чужих секретов, хакеры стремятся найти все источники конфиденциальной информации, которые могли бы найти достоверную информацию в больших объёмах за короткое время. С помощью различных уловок, множества приёмов и средств к разным источникам. Источником информации является материальный объект, обладающий определёнными сведениями, представляющий конкретный интерес для злоумышленников.

За последнее время злоупотребление информации передаваемой по каналам связи увеличивается быстрее, чем меры защиты от неё. В настоящее время для защиты информации требуется реализация системного подхода, включающего комплекс мер (специальных технических и программных средств, нормативно-правовых актов и т.д.).

1. Основные понятия информационной безопасности

В повседневной жизни часто информационная безопасность (ИБ) понимается лишь как необходимая борьба с утечкой секретной и распространением ложной и враждебной информации. А так же подразделяется на:

- надежность работы компьютера;

- сохранность ценных данных;

- защиту информации от внесения в нее изменений неуполномоченными лицами;

- сохранение тайны переписки в электронной связи.

Информация – сведения (сообщения, данные) независимо от формы

их представления.

Своевременность информации - оценивается временем выдачи (получения), в течение которого информация не потеряла свою актуальность.

Актуальность информации – это степень её соответствия текущему моменту времени. Нередко с актуальностью связывают коммерческую ценность информации. Устаревшая и потерявшая свою актуальность информация может

приводить к ошибочным решениям и тем самым теряет свою практическую ценность.

Полнота информации - определяет достаточность данных для принятия решений или для создания новых данных на основе имеющихся. Чем полнее данные, тем проще подобрать метод, вносящий минимум погрешностей в ход информационного процесса.

Достоверность информации – это степень соответствия между получаемой и исходящей информацией.

Адекватность информации – это степень соответствия реальному объективному состоянию дела. Неадекватная информация может образовываться при создании новой информации на основе неполных или недостаточных данных. Однако и полные, и достоверные данные могут приводить к созданию неадекватной информации в случае применения к ним неадекватных методов.

Доступность информации – это мера возможности получить ту или иную информацию. Отсутствие доступа к данным или отсутствие адекватных методов обработки данных приводят к одинаковому результату: информация оказывается недоступной.

Информационные технологии – процессы, методы поиска, сбора,

хранения, обработки, предоставления, распространения информации и

способы осуществления таких процессов и методов.

Информационная система – совокупность содержащейся в базах

данных информации и обеспечивающих ее обработку информационных

технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая

система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной

техники.

В утратившем силу ФЗ <<Об информации, информатизации и защите информации>> под информационной безопасностью понимается состояние защищённости информационной среды общества, обеспечивающее её формирование и развитие в интересах граждан, организаций и государства.

Информационная безопасность-это

1. комплекс организационно-технических мероприятий, обеспечивающих ценность данных и конфиденциальность информации в сочетании с её доступностью для всех авторизованных пользователей;

2. показатель, отражающий статус для всех авторизованной системы;

3. состояние защищённости информационной среды;

4. состояние, обеспечивающее защищённость информационных ресурсов и каналов, а также доступа к источникам информации.

Меры по обеспечению информационной безопасности должны осуществляться в разных сферах- политике, экономике, обороне, а также на различных уровнях- государственном, региональном, организационном и личностном.

На государственном уровне субъектами ИБ являются органы исполнительной, законодательной и судебной власти. В отдельных ведомствах созданы органы, специально занимающиеся информационной безопасностью.

Субъектами ИБ являются органы и структуры, которые в той или иной мере занимаются её обеспечением.

Кроме этого, субъектами ИБ могут быть:

-граждане и общественные объединения;

-средства массовой информации;

-предприятия и организации независимо от формы собственности.

Интересы субъектов ИБ, связанных с использованием информационных систем, можно подразделить на следующие основные категории:

Доступность - возможность за приемлемое время получить требуемую информационную услугу. Информационные системы создаются (приобретаются)

для получения определённых информационных услуг (сервисов).

Целостность - актуальность и непротиворечивость информации, её защищённость от разрушения и несанкционированного изменения. Целостность можно подразделять на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзиций)). Практически все нормативные документы и отечественные разработки относятся к статической целостности, хотя динамический аспект не менее важен.

Целостность можно подразделить на:

- **статическую,** понимаемую как неизменность информационных

объектов;

- **динамическую,** относящуюся к корректному выполнению сложных

действий. Средства контроля динамической целостности

применяются, в частности, при анализе потока финансовых

сообщений с целью выявления кражи, переупорядочения или

дублирования отдельных сообщений.

Конфиденциальность - защита от несанкционированного ознакомления. На страже конфиденциальности стоят законы, нормативные акты, многолетний опыт соответствующих служб. Аппоратно-програмные продукты позволяют закрыть практически все потенциальные каналы утечки информации.

Цели мероприятий в области информационной безопасности:

- защита интересов субъектов ИБ.

- обеспечение человека и общества достоверной и полной информацией;
- правовая защита человека и общества при получении, распространении и использовании информации.

Задачи информационной безопасности:

1. Обеспечение права личности и общества на получение информации.

2. Обеспечение объективной информацией.

3. Борьба с криминальными угрозами в сфере информационных и телекоммуникационных систем, с телефонным терроризмом, отмыванием денег и т.д.

4. Защита личности, организации, общества и государства от информационно-психологических угроз.

5. Формирование имиджа, борьбы с клеветой, слухами, дезинформацией.

Роль информационной безопасности возрастает при возникновении экстремальной ситуации, когда любое недостоверное сообщение может привести к усугублению обстановки.

Критерии ИТ - гарантированная защищённость информации от утечки, искажения, утраты или иных форм обесценивания. Безопасные информационные технологии должны обладать способностью к недопущению или нейтрализации, содержать в себе адекватные методы и способы её защиты.

Под **информационной безопасностью в широком смысле** будем

понимать такое свойство процесса информатизации и всей жизнедеятельности общества, которое гарантирует устранение всех негативных последствий информатизации, либо сводит их до такого минимума, который обеспечивает выживание и дальнейшее развитие человечества, его превращение в развитую, гуманную информационную цивилизацию.

Только в случае обеспечения информационной безопасности информатизация общества окажется процессом всеобщей интеллектуально-

гуманистической перестройки жизнедеятельности человечества на основе

наиболее полного использования информации как ресурса его развития.

Проблема информационной безопасности в своем системно-обобщенном плане в настоящее время только начинает разрабатываться в рамках нового научного направления, именуемого социальной информатикой и претендующего на изучение закономерностей взаимодействия общества и информатики, прежде всего процесса информатизации общества и становления информационной цивилизации.

Информационная безопасность в узком смысле (Information

security) – это совокупность свойств информации, связанная с обеспечением запрещения неавторизованного доступа (получения, ознакомления с содержанием, передачи, хранения и обработки), модификации или уничтожения, а также любых других несанкционированных действий с личной, конфиденциальной или секретной информацией, представленной в любом физическом виде.

По своему **содержанию** информационная безопасность включает:

1. компьютерную безопасность;

2. безопасность информационных систем и процессов в обществе

(в том числе и еще не охваченных процессом информатизации);

3. создание необходимой социальной среды для гуманистической

ориентации информационных процессов.

Защита информации – это комплекс мероприятий, направленных на

обеспечение информационной безопасности.

В государстве должна проводиться единая политика в области безопасности информационных технологий. Это требование нашло отражение в “Концепции национальной безопасности Российской Федерации”, утверждённой Указом Президента РФ № 1300 от 17 декабря 1997 года. В этом документе отмечается, что в современных условиях всеобщей информатизации и развития информационных технологий резко возрастает значение обеспечения национальной безопасности РФ в информационной сфере. Значимость обеспечения безопасности государства в информационной сфере подчёркнута и в принятой в сентябре 2000 года “Доктрине информационной безопасности Российской Федерации”. В этих документах определены важнейшие задачи государства в области информационной безопасности:

- установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями её распространения;
- совершенствование информационной структуры, ускорение развития новых информационных технологий и их широкое внедрение, унификация средств поиска, сбора, хранения и анализа информации с учётом вхождения России в

глобальную информационную инфраструктуру;
- разработка соответствующей нормативной правовой базы в интересах обеспечения информационной безопасности;
- координация деятельности органов государственной власти и других органов, решающих задачи обеспечения информационной безопасности;
- развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;
- защита государственного информационного ресурса и, прежде всего, в федеральных органах власти и на предприятиях оборонного комплекса.

25 февраля 1995 года Государственной Думой принят Федеральный закон “Об информации, информатизации и защите информации”. В законе даны определения основных терминов: информация, информатизация, информационные системы, информационные ресурсы, конфиденциальная информация, собственник и владелец информационных ресурсов, пользователь информации. Государство гарантирует права владельца информации, независимо от форм собственности, распоряжаться ею в пределах, установленных законом. Владелец информации имеет право защищать свои информационные ресурсы, устанавливать режим доступа к ним. В этом законе определены цели и режимы защиты информации, а также порядок защиты прав субъектов в сфере информационных процессов и информатизации.

Другим важным правовым документом, регламентирующим вопросы защиты информации в КС, является закон РФ “О государственной тайне”, принятый 21.07.93 года. Закон определяет уровни секретности государственной информации и соответствующую степень важности информации.

Отношения, связанные с созданием программ и баз данных, регулируются законом РФ от 23.09.92 года “О правовой охране программ для ЭВМ и баз данных” и законом РФ от 09.07.93 года “Об авторском праве и смежных правах”.

Важной составляющей правового регулирования в области информационных технологий является установление ответственности

граждан за противоправные действия при работе с КС. Преступления, совершённые с использованием КС или причинившие ущерб владельцам КС, получили название компьютерных преступлений.

В Уголовном кодексе РФ, принятом 1 января 1997 года, включена глава № 28, в которой определена уголовная ответственность за преступления в области компьютерных технологий.

В статье 272 предусмотрены наказания за неправомерный доступ к компьютерной информации. Это правонарушение может наказываться от штрафа в размере 200 минимальных зарплат до лишения свободы на срок до 5 лет.

Статья 273 устанавливает ответственность за создание, использование и распространение вредоносных программ для ЭВМ. Это правонарушение может наказываться от штрафа до лишения свободы на срок до 7 лет.

В статье 274 определена ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Если такое деяние причинило существенный вред, то виновные наказываются лишением права занимать определённые должности или заниматься определённой деятельностью на срок до 5 лет. Если те же деяния повлекли тяжкие последствия, то предусмотрено лишение свободы на срок до 4 лет.

Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации» установлено, что **защита информации** представляет собой принятие правовых, организационных и технических мер, направленных на:

1. **обеспечение защиты информации** от неправомерного доступа,

уничтожения, **модифицирования**, блокирования, копирования,

предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2. **соблюдение конфиденциальности** информации ограниченного

доступа;

3. реализацию **права на доступ** к информации.

К основным направлениям обеспечения информационной безопасности относятся:

· защита государственной тайны, т.е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения;

· защита прав граждан на владение, распоряжение и управление

принадлежащей им информацией;

· защита прав предпринимателей при осуществлении ими коммерческой деятельности;

· защита конституционных прав граждан на тайну переписки, пере-

говоров, личную тайну;

· защита технических и программных средств информатики от

ошибочных действий персонала и техногенных воздействий, а

также стихийных бедствий и иных форс-мажорных обстоятельств

с целью сохранения возможности управления процессом обработки.

1.1 Методы и средства защиты информации

В различных сферах жизнедеятельности имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности Российской Федерации.

Общие методы обеспечения информационной безопасности

Российской Федерации разделяются на правовые, организационно-технические и экономические.

К **правовым методам** обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации.

Наиболее важными направлениями этой деятельности являются:

- внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности, в

целях создания и совершенствования системы обеспечения информационной безопасности Российской Федерации, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности Российской Федерации;

законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;

- разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и

физических лиц за несанкционированный доступ к информации, ее

противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;

- уточнение статуса иностранных информационных агентств,

средств массовой информации и журналистов, а также инвесторов

при привлечении иностранных инвестиций для развития информационной инфраструктуры России;

- законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических

спутников связи;

К организационно-техническим методам обеспечения информационной безопасности Российской Федерации относятся:

- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;

- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;

- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности эти средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;

- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата

информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и

передаче по каналам связи, контроль за выполнением специальных

требований по защите информации;

- сертификация средств защиты информации, лицензирование

деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;

К экономическим методам обеспечения информационной

безопасности Российской Федерации относятся:

- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;

- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Обеспечение информационной безопасности Российской Федерации в сфере экономики играет ключевую роль в обеспечении национальной безопасности Российской Федерации.

Воздействию угроз информационной безопасности Российской Федерации в сфере экономики наиболее подвержены:

- система государственной статистики;

- кредитно-финансовая система;

- информационные и учетные автоматизированные системы под-

разделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;

- системы бухгалтерского учета предприятий, учреждений и

организаций независимо от формы собственности;

- системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

Основными мерами по обеспечению информационной безопасности Российской Федерации в сфере экономики являются:

- организация и осуществление государственного контроля за

созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

- коренная перестройка системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации, организацию контроля за деятельностью этих лиц и служб обработки и анализа статистической информации, а также путем ограничения коммерциализации такой информации;

- разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

- разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация этих систем, а также разработка нормативной правовой базы, регламентирующей их использование;

- совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;

- совершенствование методов отбора и подготовки персонала

для работы в системах сбора, обработки, хранения и передачи экономической информации.

«Режим защиты информации устанавливается:

- в отношении сведений, отнесенных к государственной тайне, -

уполномоченными органами на основании Закона Российской

Федерации «О государственной тайне»;

- в отношении конфиденциальной документированной информации -

собственником информационных ресурсов или уполномоченным

лицом на основании настоящего Федерального закона;

- в отношении персональных данных - федеральным законом.»

Система защиты информации – рациональная совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятству-

ющих несанкционированному доступу к информации, ее разглашению или утечке.

Основной характеристикой системы является ее комплексность, т. е. наличие в ней обязательных элементов, охватывающих все направления защиты информации. Элементами системы являются: правовой, организационный, инженерно-технический, программно-аппаратный и криптографический.

Правовой элемент системы защиты информации основывается на нормах информационного права и предполагает юридическое закрепление взаимоотношений фирмы и государства по поводу правомерности использования системы защиты информации.

Организационный элемент системы защиты информации содержит меры управленческого, ограничительного (режимного) и технологического характера, определяющие основы и содержание системы защиты, побуждающие персонал соблюдать правила защиты конфиденциальной информации фирмы.

Инженерно-технический элемент системы защиты информации предназначен для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, здания, помещений и оборудования с помощью комплексов технических средств.

Программно-аппаратный элемент системы защиты информации предназначен для защиты ценной информации, обрабатываемой и хранящейся в компьютерах, серверах и рабочих станциях локальных сетей и различных информационных системах.

Криптографический элемент системы защиты информации предназначен для защиты конфиденциальной информации методами криптографии. Элемент включает:

регламентацию использования различных криптографических методов в ЭВМ и локальных сетях;

- определение условий и методов криптографирования текста документа при передаче его по незащищенным каналам почтовой, телеграфной, телетайпной, факсимильной и электронной связи;

- регламентацию использования средств криптографирования переговоров по незащищенным каналам телефонной и радиосвязи;

- регламентацию доступа к базам данных, файлам, электронным документам пер сональными паролями, идентифицирующими командами и другими методами;

- регламентацию доступа персонала в выделенные помещения с помощью идентифицирующих кодов, шифров.

Система защиты информации, как любая система, должна иметь определенные виды собственного обеспечения, опираясь на которые она будет выполнять свою целевую функцию. С учетом этого система защиты информации может иметь: **Правовое обеспечение -** сюда входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы действия; **Организационное обеспечение -** имеется в виду, что реализация защиты информации осуществляется определенными структурными единицами, такими как: служба безопасности, служба режима, служба защиты информации техническими средствами и др. **Аппаратное обеспечение** - предполагается широкое использование технических средств, как для защиты информации, так и для обеспечения деятельности собственно системы защиты информации; **Информационное обеспечение** - оно включает в себя документированные сведения (показатели, файлы), лежащие в основе решения задач, обеспечивающих функционирование системы. Сюда могут входить как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности; **Программное обеспечение -** к нему относятся антивирусные программы, а также программы (или части программ регулярного применения), реализующие контрольные функции при решении учетных, статистических, финансовых, кредитных и других задач; **Математическое обеспечение** - предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты; **Лингвистическое обеспечение -** совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации; **Нормативно-методическое обеспечение** - сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации; **Эргономическое обеспечение -** совокупность средств, обеспечивающих удобства работы пользователей аппаратных средств защиты информации. **Особенностью системного подхода** к защите информации является создание защищенной среды

обработки, хранения и передачи информации, объединяющей разнородные методы и средства противодействия угрозам: программно-технические, правовые, организационно-экономические. Организация подобной защищенной среды позволяет гарантировать определенный уровень безопасности автоматизированной информационной системы. **Системный подход к защите информации базируется на следующих методологических принципах:**

1. конечная цель - абсолютного приоритета конечной (глобальной) цели;

2. единства - совместного рассмотрения системы как целого так и совокупность частей (элементов);

3. связанности - рассмотрения любой части системы совместного с её связями с окружением;

4. модельного построения - выделения модулей в системе и рассмотрения её как совокупности моделей;

5. иерархия - введения иерархии частей (элементов) и их ранжирования;

6. функциональности - совместного рассмотрения структуры и функции с приоритетом функции над структурой;

7. развития - учета изменяемости системы, её способности к развитию, расширению, замене частей, накапливанию информации;

8. децентрализации - сочетания в принимаемых решениях и управлении централизацию, замена частей, накапливанию информации;

9. неопределенности - учета неопределенностей и случайностей в системе.

Каждую систему защиты следует разрабатывать индивидуально, учитывая следующие особенности:

1. организационную структуру организации;

2. объем и характер информационных потоков (внутри объекта в целом, внутри отделов, между отделами, внешних);

3. количество и характер выполняемых операций: аналитических и повседневных;

4. количество и функциональные обязанности персонала;

5. количество и характер клиентов;

6. график суточной нагрузки.

Защита должна разрабатываться для каждой системы индивидуально, но в соответствии с общими правилами. Построение защиты предполагает следующие этапы:

1. анализ риска, заканчивающийся разработкой проекта системы защиты и планов защиты, непрерывной работы и восстановления;

2. реализация системы защиты на основе результатов анализа риска;

3. постоянный контроль за работой системы защиты и АИС в целом (программный, системный и административный).

На каждом этапе реализуются определенные требования к защите; их точное соблюдение приводит к созданию безопасной системы.

Методы и средства защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам. Эффективность информационной безопасности означает, что затраты на ее осуществление не должны быть больше возможных потерь от реализации информационных угроз. Планирование безопасности информации осуществляется путем разработки каждой службой детальных планов защиты информации. Необходима четкость в осуществлении полномочий и прав пользователей на доступ к определенным видам информации.

Препятствие - метод физической преграды на пути злоумышленников к защищенной информации.

Управление доступом - методы защиты информации используя все ресурсы ИС и ИТ. Эти методы противостоят всем несанкционированным доступам к информации.

Механизмы шифрования - криптографическое закрытие информации.

2. Угрозы информационной безопасности

2.1 Понятие и классификация угроз информационной безопасности

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность.

К основным угрозам информационной безопасности относятся:

- утечка конфиденциальной информации;
- несанкционированное использование информационных ресурсов;
- несанкционированный обмен информации между абонентами;
- отказ от информации;
- нарушение информационного обслуживания.

Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку - **злоумышленником**. Потенциальные злоумышленники называются **источниками угрозы**.

По цели воздействия различают три основных типа угроз безопасности автоматизированной системы обработки информации:

- угрозы нарушения конфиденциальности информации;
- угрозы нарушения целостности информации;
- угрозы нарушения работоспособности системы (отказы в обслуживании).

Угрозы нарушения конфиденциальности направлены на разглашение конфиденциальной или секретной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ.

Угрозы нарушения целостности информации, хранящейся в

компьютерной системе или передаваемой по каналу связи, направлены на ее

изменение или искажение, приводящее к нарушению ее качества или полному уничтожению.

Угрозы нарушения работоспособности (отказ в обслуживании)

направлены на создание таких ситуаций, когда определенные

преднамеренные действия либо снижают работоспособность автоматизированной системы обработки информации, либо

блокируют доступ к некоторым ее ресурсам.

Автоматизированная система обработки информации состоит из следующих компонент:

- **аппаратные средства** — ЭВМ и их составные части (процессоры,

мониторы, терминалы, периферийные устройства-дисководы,

принтеры, контроллеры, кабели, линии связи) и т.д.;

- **программное обеспечение** — приобретенные программы, исходные,

объектные, загрузочные модули; операционные системы и

системные программы (компиляторы, компоновщики и др.),

утилиты, диагностические программы и т.д.;

- **данные** — хранимые временно и постоянно, на магнитных

носителях, печатные, архивы, системные журналы и т.д.;

- **персонал** — обслуживающий персонал и пользователи.

Практически каждый компонент может подвергнуться внешнему

воздействию или выйти из строя.

Опасные воздействия на автоматизированную систему обработки информации можно подразделить на:

- случайные;

- преднамеренные.

Случайные воздействия. Анализ опыта проектирований, изготовления

и эксплуатации автоматизированной системы обработки информации показывает, что информация подвергается различным

случайным воздействиям на всех этапах цикла жизни и функционирования

автоматизированная система обработки информации.

Причинами случайных воздействий при эксплуатации автоматизированная система обработки информации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений

электропитания;

- отказы и сбои аппаратуры;

- ошибки в программном обеспечении;

- ошибки в работе обслуживающего персонала и пользователей;

- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные угрозы связаны с целенаправленными действиями

нарушителя. В качестве нарушителя могут выступать служащий, посетитель,

конкурент, наемник и т.д.

Действиями нарушителя, можно составить **гипотетическую**

модель потенциального нарушителя:

1. квалификация нарушителя может быть на уровне разработчика

данной системы;

2. нарушителем может быть как постороннее лицо, так и законный

пользователь системы;

3. нарушителю известна информация о принципах работы системы;

4. нарушитель выберет наиболее слабое звено в защите.

Угрозы информационной безопасности – события или действия, которые могут привести к искажению, неразрешенному использованию или к разрушению информационных ресурсов управления системы, а также программных и аппаратных средств.

1. Проблемы, связанные с информационной безопасностью,

для разных категорий субъектов может существенно различаться.

В первом случае «пусть лучше все сломается, чем враг узнает хоть один

секретный бит», во втором – «да нет у нас никаких секретов, лишь

бы все работало».

2. Информационная безопасность не сводится исключительно к защите

от несанкционированного доступа к информации, это

принципиально более широкое понятие. Субъект информационных

отношений может пострадать (понести убытки и/или получить

моральный ущерб) не только от несанкционированного доступа, но

и от поломки системы, вызвавшей перерыв в работе.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации: информационные, программные, физические, радиоэлектронные и организационно-правовые.

К **информационным** угрозам относятся:

- несанкционированный доступ к информационным ресурсам;

- незаконное копирование данных в информационных системах;

- хищение информации из библиотек, архивов, банков и баз данных;

- нарушение технологии обработки информации;

- противозаконный сбор и использование информации;

- использование информационного оружия.

К **программным** угрозам относятся:

- использование ошибок и <<дыр>> в программном обеспечении;

- компьютерные вирусы и вредоносные программы;

- установка <<закладных>> устройств.

К **физическим** угрозам относятся:

- уничтожение или разрушение средств обработки информации и связи;

- хищение носителей информации;

- хищение программных или аппаратных ключей и средств криптографической защиты данных;

- воздействие на персонал.

К **радиоэлектронным** угрозам относятся:

- внедрение электронных устройств перехвата информации в технические средства и помещения;

- перехват, расшифровка, подмена и уничтожение информации в каналах связи.

К **организационно-правовым** угрозам относятся:

- нарушение требований законодательства и задержка в принятии необходимых нормативно-правовых решений в информационной сфере;

- закупка несовершенных или устаревших информационных технологий и средств информатизации.

2.2 Виды информационных угроз безопасности

К видом информационных угроз безопасности относятся:

· нарушение технологии и обработки информации;

· утечка информации по техническим каналам;

· использование не сертифицированных средств информационной

инфраструктуры;

· противоправные сбор и использование информации;

· внедрение в аппаратные средства и программные изделия нерегламентированных компонентов;

· внедрение электронных устройств перехвата информации в помещения и системы;

· уничтожение, повреждение, радиоэлектронное подавление или

разрушение средств информационной инфраструктуры;

· навязывание ложной информации.

Целевая характеристика угроз информационной безопасности

· Ознакомление (получение) – противоправное действие, не приводящее к изменению или разрушению информации.

· Искажение (модификация) – случайные или преднамеренные действия, приводящие к частичному изменению содержания.

· Разрушение (уничтожение) – противоправные действия, приводящие к значительному или полному разрушению информационных ресурсов

Каналы утечки информации

Применительно к практике с учетом физической природы образования **каналы утечки** информации можно разделить на следующие группы:

· визуально-оптические;

· акустические (включая и акустико-преобразовательные);

· электромагнитные (включая магнитные и электрические);

· материально-вещественные (бумага, фото, магнитные носители, производственные отходы различного вида).

По механизму распространения различают:

- **вирусы** - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;

- **«черви»** - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. «Черви», напротив, ориентированы в первую очередь на распространение по сети.

Вредоносный код, который выглядит как функционально полезная программа, называется **троянским вирусом**.

«**Программный вирус** - это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах».

Классификация вредоносных программ:

- логические бомбы;

- троянский конь;

- компьютерный вирус;

- червь;

- захватчик паролей.

Логические бомбы – это программы или их части, постоянно находящиеся в ЭВМ или вычислительных систем (КС) и выполняемые только при соблюдении определённых условий.

Троянский конь – это программа, полученная путём явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.

Компьютерный вирус – это небольшая программа, которая после внедрения в ЭВМ самостоятельно распространяются путём создания своих копий, а при выполнении определённых условий оказывают негативное воздействие на КС.

Вирус - программа, которая заражает другие программы включая в них модифицированную копию, обладает дальнейшим размножением.

Вирус характеризуется двумя способами:

1. способность к саморазмножению;

2. способен вмешиваться в вычислительный процесс.

Червь - программа, распространяется через сеть и не оставляет своей копии на магнитном носителе. Способ защиты от червя - принять меры против несанкционированного доступа к сети.

Захватчик паролей - программы, предназначены для воровства паролей.

Виды умышленных угроз информационной безопасности:

Пассивные угрозы направлены на несанкционированное использование информационных ресурсов ИС, не влияя на её функционирование.

Активные угрозы нарушают функционирование ИС путем целенаправленного воздействия на её компоненты. Источником активных угроз это действие хакеров, вредоносных программ и т.д.

Источники угроз информационной безопасности

Внешние:

1. Компьютерные вирусы и вредоносные программы;

2. Организация и отдельные лица;

3. Стихийные бедствия.

Формами проявления внешних угроз являются:

- заражение компьютеров вирусами или вредоносными программами;

- несанкционированный доступ к корпоративной информации;

- информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;

- действия государственных структур и служб, уничтожением информации.

Внутренние:

1. Сотрудники организации;

2. Программное обеспечение;

3. Аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

-ошибки пользователей и системных администраторов;

- нарушения сотрудниками фирмы установленных регламентов сбора, обработки и уничтожения информации;

- ошибки в работе программного обеспечения;

- отказы и сбои в работе программного обеспечения.

2.3. Криптографические методы зашиты информации

Готовое к передаче информационное сообщение, первоначально открытое и незащищенное, зашифровывается и тем самым преобразуется в шифрограмму, т. е. в закрытые текст или графическое изображение документа. В таком виде сообщение передается по каналу связи, даже и не защищенному. Санкционированный пользователь после получения сообщения дешифрует его (т. е. раскрывает) посредством обратного преобразования криптограммы, вследствие чего получается исходный, открытый вид сообщения, доступный для восприятия санкционированным пользователям.

Методу преобразования в криптографической системе соответствует использование специального алгоритма. Действие такого алгоритма запускается уникальным числом (последовательностью бит), обычно называемым шифрующим ключом.

Для большинства систем схема генератора ключа может представлять собой набор инструкций и команд либо узел аппаратуры, либо компьютерную программу, либо все это вместе, но в любом случае процесс шифрования (дешифрования) реализуется только этим специальным ключом. Чтобы обмен зашифрованными данными проходил успешно, как отправителю, так и получателю, необходимо знать правильную ключевую установку и хранить ее в тайне.

Стойкость любой системы закрытой связи определяется степенью секретности используемого в ней ключа. Тем не менее этот ключ должен быть известен другим пользователям сети, чтобы они могли свободно обмениваться зашифрованными сообщениями. В этом смысле криптографические системы также помогают решить проблему аутентификации (установления подлинности) принятой информации. Взломщик в случае перехвата сообщения будет иметь дело только с зашифрованным текстом, а истинный получатель, принимая сообщения, закрытые известным ему и отправителю ключом, будет надежно защищен от возможной дезинформации.

Современная криптография знает два типа криптографических алгоритмов: классические алгоритмы, основанные на использовании закрытых, секретных

ключей, и новые алгоритмы с открытым ключом, в которых используются один открытый и один закрытый ключ (эти алгоритмы называются также асимметричными). Кроме того, существует возможность шифрования информации и более простым способом — с использованием генератора псевдослучайных чисел.

Использование генератора псевдослучайных чисел заключается в генерации гаммы шифра с помощью генератора псевдослучайных чисел при определенном ключе и наложении полученной гаммы на открытые данные обратимым способом.

Надежность шифрования с помощью генератора псевдослучайных чисел зависит как от характеристик генератора, так и, причем в большей степени, от алгоритма получения гаммы.

Этот метод криптографической защиты реализуется достаточно легко и обеспечивает довольно высокую скорость шифрования, однако недостаточно стоек к дешифрованию и поэтому неприменим для таких серьезных информационных систем, каковыми являются, например, банковские системы.

Для классической криптографии характерно использование одной секретной единицы — ключа, который позволяет отправителю зашифровать сообщение, а получателю расшифровать его. В случае шифрования данных, хранимых на магнитных или иных носителях информации, ключ позволяет зашифровать информацию при записи на носитель и расшифровать при чтении с него.

Существует довольно много различных алгоритмов криптографической защиты информации. Среди них можно назвать алгоритмы DES, Rainbow **(CIIJA); FEAL-4 и FEAL-8** (Япония); B-Crypt (Великобритания); алгоритм шифрования по **ГОСТ** 28147 — 89 (Россия) и ряд других, реализованных зарубежными и отечественными поставщиками программных и аппаратных средств защиты

Наиболее перспективными системами криптографической защиты данных сегодня считаются асимметричные криптосистемы, называемые также системами с открытым ключом. Их суть состоит в том, что ключ, используемый для зашифровывания, отличен от ключа расшифровывания. При этом ключ зашифровывания не секретен и может быть известен всем пользователям системы. Однако расшифровывание с помощью известного ключа зашифровывания невозможно. Для расшифровывания используется специальный, секретный ключ. Знание открытого ключа не позволяет определить ключ секретный. Таким образом, расшифровать сообщение может только его получатель, владеющий этим секретным ключом.

Суть криптографических систем с открытым ключом сводится к тому, что в них используются так называемые необратимые функции (иногда их называют односторонними или однонаправленными), которые характеризуются следующим свойством: для данного исходного значения с помощью некоторой известной функции довольно легко вычислить результат, но рассчитать по этому результату исходное значение чрезвычайно сложно.

Известно несколько криптосистем с открытым ключом. Наиболее разработана на сегодня система RSA. RSA— это система коллективного пользования, в которой каждый из пользователей имеет свои ключи зашифровывания и расшифровывания данных, причем секретен только ключ расшифровывания.

Специалисты считают, что системы с открытым ключом больше подходят для шифрования передаваемых данных, чем для защиты данных, хранимых на носителях информации. Существует еще одна область применения этого алгоритма — цифровые подписи, подтверждающие подлинность передаваемых документов и сообщений.

Асимметричные криптосистемы наиболее перспективны, так как в них не используется передача ключей другим пользователям и они легко реализуются как аппаратным, так и программным способами. Однако системы типа RSA работают приблизительно в тысячу раз медленнее, чем классические, и требуют длины ключа порядка 300— 600 бит. Поэтому все их достоинства сводятся на нет низкой скоростью работы. Кроме того, для ряда функций найдены алгоритмы инвертирования, т. е. доказано, что они не являются необратимыми. Для функций, используемых в системе RSA, такие алгоритмы не найдены, но нет и строгого доказательства необратимости используемых функций. В последнее время все чаще возникает вопрос о замене в системах передачи и обработки информации рукописной подписи, подтверждающей подлинность того или иного документа, ее электронным аналогом — электронной цифровой подписью (ЭЦП). Ею могут скрепляться всевозможные электронные документы, начиная с различных сообщений и кончая контрактами. ЭЦП может применяться также для контроля доступа к особо важной ин- формации. К ЭЦП предъявляются два основных требования: высокая сложность фальсификации и легкость проверки.

Для реализации ЭЦП можно использовать как классические криптографические алгоритмы, так и асимметричные, причем именно последние обладают всеми свойствами, необходимыми для ЭЦП.

Однако ЭЦП чрезвычайно подвержена действию обобщенного класса программ «троянский конь» с преднамеренно заложенными в них потенциально опасными последствиями, активизирующимися при определенных условиях. Например, в момент считывания файла, в котором находится подготовленный к подписи документ, эти программы могут изменить имя подписывающего лица, дату, какие-либо данные (например, сумму в платежных документах) и т.п.

Поэтому при выборе системы ЭЦП предпочтение безусловно должно быть отдано ее аппаратной реализации, обеспечивающей надежную защиту информации от несанкционированного доступа, выработку криптографических ключей и ЭЦП.

Из изложенного следует, что надежная криптографическая система должна удовлетворять ряду определенных требований.

• Процедуры зашифровывания и расшифровывания должны быть «прозрачны» для пользователя.

• Дешифрование закрытой информации должно быть максимально затруднено.

• Содержание передаваемой информации не должно сказываться на эффективности криптографического алгоритма.

• Надежность криптозащиты не должна зависеть от содержания в секрете самого алгоритма шифрования (примерами этого являются как алгоритм DES, так и алгоритм ГОСТ 28147 — 89).

Процессы защиты информации, шифрования и дешифрования связаны с кодируемыми объектами и процессами, их свойствами, особенностями перемещения. Такими объектами и процессами могут быть материальные объекты, ресурсы, товары, сообщения, блоки информации, транзакции (минимальные взаимодействия с базой данных по сети). Кодирование кроме целей защиты, повышая скорость доступа к данным, позволяет быстро определять и выходить на любой вид товара и продукции, страну-производителя и т.д. В единую логическую цепочку связываются операции, относящиеся к одной сделке, но географически разбросанные по сети.

Например, штриховое кодирование используется как разновидность автоматической идентификации элементов материальных потоков, например товаров, и применяется для контроля за их движением в реальном времени. Достигается оперативность управления потоками материалов и продукции,

повышается эффективность управления предприятием. Штриховое кодирование позволяет не только защитить информацию, но и обеспечивает высокую скорость чтения и записи кодов. Наряду со штриховыми кодами в целях за- щиты информации используют голографические методы.

Методы защиты информации с использованием голографии являются актуальным и развивающимся направлением. Голография представляет собой раздел науки и техники, занимающийся изучением и созданием способов, устройств для записи и обработки волн различной природы. Оптическая голография основана на явлении интерференции волн. Интерференция волн наблюдается при распределении в пространстве волн и медленном пространственном распределении результирующей волны. Возникающая при интерференции волн картина содержит информацию об объекте. Если эту картину фиксировать на светочувствительной поверхности, то образуется голограмма. При облучении голограммы или ее участка опорной волной можно увидеть объемное трехмерное изображение объекта. Голография применима к волнам любой природы и в настоящее время находит все большее практическое применение для идентификации продукции различного назначения.

Технология применения кодов в современных условиях преследует цели защиты информации, сокращения трудозатрат и обеспечение быстроты ее обработки, экономии компьютерной памяти, формализованного описания данных на основе их систематизации и классификации.

В совокупности кодирование, шифрование и защита данных предотвращают искажения информационного отображения реальных производственно-хозяйственных процессов, движения материальных, финансовых и других потоков, а тем самым способствуют обоснованности формирования и принятия управленческих решений.

Заключение

Рассматривая всё, очевидно, что информационная безопасность является комплексной задачей. Нужно четко представлять себе, что ни какие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных. Информационная среда является сложным

механизмом, в который входят такие компоненты, как электронные оборудования, программное обеспечение и т.д.

Необходимое решение проблем обеспечения информационной безопасности должны применяться меры законодательные, организационные и програмно-технические. Пренебрежение одного из аспектов проблем приводит к утрате или утечки информации.

Использование высокоэффективных информационных систем является обязательным условием успешной деятельности современных организаций и предприятий. Безопасность информации — это один из основных показателей качества информационной системы. Обеспечение информационной безопасности - дорогое дело. Большая концентрация защитных средств в информационной системе может привести к тому, что система окажется очень дорого стоящей, потому нерентабельной и неконкурентоспособной, но и к тому, что у нее произойдет существенное снижение коэффициента готовности. Так же стоит обратить большое внимание на внешние и внутренние угрозы. Главное при определении мер и принципов защиты информации это квалифицированно определить границы безопасности и затраты на средства защиты с одной стороны поддержание системы в работоспособном состоянии и приемлемом риске с другой стороны.

Список литературы

1. Гафнер В. В. Информационная безопасность. Учебное пособие. Ростов н/Д: Феникс,2010.-324с.

2. Котухов М. М., Кубанков А. Н., Калашников А. О. Информационная безопасность. Учебное пособие. – М.: Академия ИБС: МФТИ, 2009. – 195 с.

3. Сычев Ю.Н. ОСНОВЫ ИНФОРМАЦИОННАЯ БЕЗОПАС-

НОСТЬ. Учебно-практическое пособие. – М.: Изд. центр ЕАОИ, 2007. –

300 с.

4. Макаренко С. И. Информационная безопасность: учебное пособие для

студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. –

372 с.: ил.

5. Артёмов А. Информационная безопасность. Курс лекций.

6. Ясенев В.Н. Информационная безопасность в экономических системах. Учебно-методическое пособие.