Политика

информационной безопасности

ООО «СМК РЕСО-Мед»

г.Москва, 2014

Содержание:

1. Введение

Развитие и распространение информационных технологий, обострение конкурентной борьбы и криминогенной обстановки, требуют создания целостной системы информационной безопасности, взаимоувязывающей правовые, оперативные, технологические, организационные, технические и физические меры защиты информации.

Настоящая Политика определяет систему взглядов на проблему обеспечения информационной безопасности в единой информационной телекоммуникационной системе (далее – автоматизированной системе) Общества с ограниченной ответственностью «Страховая медицинская компания РЕСО-Мед» (далее – Общество).

2. Общие положения

2.1 Назначение и правовая основа документа

Настоящая «Политика информационной безопасности Общества» (далее – Политика) представляет собой официально принятую систему взглядов на проблему обеспечения информационной безопасности в автоматизированных системах (АС) Общества. Политика содержит систематизированное изложение целей и задач защиты, основных принципов и способов достижения требуемого уровня информационной безопасности, организационных, технологических и процедурных аспектов обеспечения информационной безопасности в АС.

Политика учитывает современное состояние и ближайшие перспективы развития АС, цели, задачи и правовые основы её создания и эксплуатации, режимы функционирования данной системы, а также анализа угроз безопасности для информационных ресурсов Общества.

Правовой основой настоящей Политики являются:

- Конституция Российской Федерации;
- Гражданский и Уголовный кодексы;
- Кодекс об административных правонарушениях;
- законы, указы, постановления и другие нормативные документы действующего законодательства Российской Федерации;
- нормативные документы федерального и территориальных фондов обязательного медицинского страхования, министерств здравоохранения и социального развития, Федеральной службы страхового надзора и др.;
- нормативные и регламентирующие документы государственных органов Российской Федерации (ФСТЭК, ФСБ, Роскомнадзор и др.);

- внутренние нормативно-методические и организационно-распорядительные документы Общества.

Основные положения и требования Политики распространяются на все структурные подразделения Общества, в которых осуществляется автоматизированная и смешанная обработка информации, содержащей сведения, составляющие коммерческую, служебную, врачебную тайну или персональные данные, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования АС. Основные положения Политики могут быть распространены также на подразделения других организаций и учреждений, осуществляющие взаимодействующие с АС в качестве поставщиков и потребителей (пользователей) информации АС.

Политика является методологической основой для:

- формирования и проведения единой политики в области информационной безопасности в АС;
- разработки стратегии информационной безопасности Общества, включая цели, задачи и комплекс мер по её практической реализации;
- принятия управленческих решений и разработки практических мер по воплощению политики информационной безопасности и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз информационной безопасности;
- координации деятельности структурных подразделений Общества при проведении работ по созданию, развитию и эксплуатации АС с соблюдением требований информационной безопасности;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения информационной безопасности АС.

Политика не регламентирует вопросы организации охраны помещений и обеспечения сохранности и физической целостности компонентов АС, защиты от стихийных бедствий, сбоев в системе энергоснабжения, а также меры по обеспечению личной безопасности персонала и клиентов Общества. Однако она предполагает построение системы информационной безопасности на тех же концептуальных основах, что и система безопасности Общества в целом (имущественная, физическая и т.д.). Это позволяет не только принципиально, но и практически сопрягать их, оптимизируя затраты на построение такой системы.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения информационной безопасности, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам информационной безопасности, а также текущее состояние и перспективы развития информационных технологий.

3. Объекты защиты

Объекты информационной безопасности – это компоненты информационной среды, угрозы которым представляют опасность для застрахованных, страхователей, работников, акционеров Общества и т.д. Основными объектами информационной безопасности в Обществе являются:

- информационные ресурсы с ограниченным доступом, составляющие коммерческую, врачебную, служебную тайну, персональные данные, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, в том числе открытая (общедоступная) информация, представленные в виде документов и массивов информации, независимо от формы и вида их представления;
- процессы обработки информации в АС – информационные технологии, регламенты и

процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков, администраторов и пользователей АС;

- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные компоненты АС.

3.1 Назначение, цели создания и эксплуатации АС как объекта информатизации

АС предназначены для автоматизации деятельности работников Общества. Создание и применение АС преследует следующие цели:

- повышение качества управления бизнес-процессами;
- повышение качества контроля движения информационных, материальных и финансовых ресурсов Общества;
- повышение оперативности и достоверности процедур сбора данных о состоянии материальных и финансовых ресурсов Общества;
- сокращение финансовых и временных затрат на поддержку внутреннего и внешнего документооборота;
- повышение оперативности и обоснованности прогнозирования коммерческой деятельности Общества;
- повышение оперативности и обоснованности планирования расходов финансовых ресурсов Общества и т.д.

А также обеспечения следующих основных процессов:

- интегрированной обработки информации, формирования и ведения специализированных баз данных;
- взаимодействия с клиентами Общества и другими внешними организациями;
- информационно-справочного обслуживания структурных подразделений Общества;
- анализа и прогнозирования деятельности Общества, обоснования принятия управленческих решений.

3.2 Структура, состав и размещение основных элементов АС, информационные связи с другими объектами

АС представляют собой системы (подсистемы) центрального и территориальных подразделений Общества, связанные между собой посредством информационно-телекоммуникационной сети общего пользования.

В различных АС циркулирует информация разных категорий. Конфиденциальная информация может совместно использоваться различными пользователями локальной вычислительной сети структурных подразделений Общества.

В ряде АС предусмотрено взаимодействие с внешними (государственными и коммерческими) организациями по коммутируемым и выделенным каналам с использованием средств передачи информации.

Комплекс технических средств АС включает средства обработки данных (ПЭВМ, серверы и т.п.), средства обмена данными в ЛВС с возможностью выхода в глобальные сети (кабельная система, модемы и т.д.), а также средства хранения (в т.ч. архивирования) данных.

К основным особенностям функционирования АС, относятся:

- территориальная распределённость ряда автоматизированных систем;

- объединение в АС технических средств обработки и передачи информации;
- разнородность решаемых задач и типов обрабатываемых данных, смешанная (ручная и автоматизированная) обработка информации с совмещением выполнения информационных запросов различных пользователей;
- объединение в ряде баз данных информации различного назначения, принадлежности и уровней конфиденциальности;
- непосредственный доступ к вычислительным и информационным ресурсам различных категорий пользователей (источников и потребителей информации);
- наличие нескольких каналов взаимодействия с «внешним миром» (источниками и потребителями информации);
- отсутствие необходимости в непрерывном функционировании АС;
- невысокая интенсивность информационных потоков в АС;
- наличие АС с различными требованиями по уровням защищенности (физически не объединенных в единую сеть);
- разнообразие категорий пользователей АС.

Общая структурная и функциональная организация АС определяется организационно-штатной структурой Общества и задачами, решаемыми его структурными подразделениями с применением средств автоматизации. В самом общем виде, единая телекоммуникационная информационная система Общества представляет собой совокупность локальных вычислительных сетей (ЛВС) филиалов Общества, объединенных средствами телекоммуникации. Каждая ЛВС в АС объединяет ряд взаимосвязанных и взаимодействующих автоматизированных подсистем (технологических участков), обеспечивающих решение задач в отдельных структурных подразделениях Общества.

Объекты информатизации АС включают:

- технологическое оборудование (средства вычислительной техники, сетевое и кабельное оборудование);
- информационные ресурсы, в том числе содержащие сведения ограниченного распространения и представленные в виде документов или записей в носителях на магнитной, оптической и другой основе, массивах и базах данных;
- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение);
- автоматизированные системы связи и передачи данных (средства телекоммуникации);
- каналы связи, по которым передается информация (в том числе ограниченного распространения);
- служебные помещения, в которых циркулирует информация (в том числе ограниченного распространения);
- технические средства и системы, не обрабатывающие информацию (вспомогательные технические средства и системы – ВТСС), размещенные в помещениях, где обрабатывается информация, содержащая сведения ограниченного распространения.

Обеспечение функционирования и эксплуатация АС осуществляется отделом информационного обеспечения Общества и подразделениями (службами, отделами, группами и отдельными сотрудниками) информационного обеспечения (информационных технологий, автоматизации) филиалов Общества (далее – ИТ-подразделения) на основании требований организационно-распорядительных документов руководства Общества и вышестоящих инстанций (ТФОМС, Министерств здравоохранения и др.).

3.3 Категории информационных ресурсов, подлежащих защите

В АС циркулирует информация различных уровней конфиденциальности, содержащая

сведения ограниченного распространения (коммерческая, врачебная тайна, персональные данные) а также общедоступные сведения.

В документообороте АС присутствуют:

- платежные поручения и другие расчетно-денежные документы;
- отчеты (бухгалтерские, управленческие и др.);
- сведения о выданных страховых медицинских полисах;
- сведения о взаиморасчетах за пролеченных пациентов;
- сведения о качестве оказанной медицинской помощи;
- обобщенная информация и другие документы.
- и т.д.

В соответствии с федеральным законом № 149-ФЗ от 27.07.2006 «Об информации, информатизации и защите информации» защите подлежит вся информация, циркулирующая в АС, содержащая конфиденциальную информацию:

- сведения, составляющие коммерческую тайну, доступ к которым ограничен собственником информации (Обществом) в соответствии с правами, предоставленными Федеральным законом № 98-ФЗ от 29.07.04 «О коммерческой тайне»;
- персональные данные физических лиц, доступ к которым ограничен в соответствии с Федеральным законом № 152-ФЗ от 27 июля 2006 г. «О персональных данных»;
- сведения, составляющие врачебную тайну, доступ к которым ограничен в соответствии с Приказом Федерального фонда ОМС от 25.03.98 № 30 «О соблюдении конфиденциальности сведений, составляющих врачебную тайну».

3.4 Категории пользователей АС, режимы использования и уровни доступа к информации

В Обществе имеются несколько категорий пользователей, которые должны иметь различные полномочия по доступу к информационным ресурсам АС:

- пользователи баз данных (конечные пользователи, работники подразделений Общества);
- ответственные за ведение баз данных (ввод, корректировка, удаление данных в БД);
- администраторы серверов (файловых серверов, серверов приложений, серверов баз данных) и ЛВС;
- системные программисты (ответственные за сопровождение общего программного обеспечения) на серверах и рабочих станциях пользователей;
- разработчики прикладного программного обеспечения;
- специалисты по обслуживанию технических средств вычислительной техники;
- администраторы информационной безопасности и др.

3.5 Уязвимость основных компонентов АС

Наиболее доступными и уязвимыми компонентами АС являются рабочие станции – автоматизированные рабочие места (АРМ) работников подразделений Общества. Именно с них могут быть предприняты наиболее многочисленные попытки несанкционированного доступа к информации (НСД) и попытки совершения несанкционированных действий (непреднамеренных и умышленных). С рабочих станций осуществляется управление процессами обработки информации (в том числе на серверах), запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На мониторы и печатающие устройства рабочих станций выводится информация при работе пользователей, выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы. Нарушения конфигурации аппаратно-программных средств рабочих станций и неправомерное вмешательство в процессы их функционирования

могут приводить к блокированию информации, невозможности своевременного решения важных задач и выходу из строя отдельных АРМ и подсистем.

В особой защите нуждаются такие элементы сетей как выделенные файловые серверы, серверы баз данных и серверы приложений. Здесь злоумышленники, прежде всего, могут искать возможности получения доступа к защищаемой информации и оказания влияния на работу различных подсистем серверов, используя недостатки протоколов обмена и средств разграничения удаленного доступа к ресурсам серверов. При этом могут предприниматься попытки как удаленного (со станций сети) так и непосредственного (с консоли сервера) воздействия на работу серверов и их средств защиты.

Мосты, шлюзы и другие сетевые устройства, каналы и средства связи также нуждаются в защите. Они могут быть использованы нарушителями для реструктуризации и дезорганизации работы сети, перехвата передаваемой информации, анализа трафика и реализации других способов вмешательства в процессы обмена данными.

4. Цели и задачи обеспечения информационной безопасности

4.1 Интересы затрагиваемых при эксплуатации АС субъектов информационных отношений

Субъектами правоотношений при использовании АС и обеспечении информационной безопасности являются:

- Общество как собственник информационных ресурсов;
- ИТ-подразделения Общества, обеспечивающие эксплуатацию систем смешанной обработки информации;
- должностные лица и работники структурных подразделений Общества, как пользователи и поставщики информации в АС в соответствии с возложенными на них функциями;
- юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в АС;
- другие юридические и физические лица, задействованные в процессе создания и функционирования АС (разработчики компонентов АС, обслуживающий персонал, организации, привлекаемые для оказания услуг в области безопасности, информационных технологий и др.).

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- конфиденциальности (сохранения в тайне) определенной части информации;
- достоверности (полноты, точности, адекватности, целостности) информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);
- своевременного доступа (за приемлемое для них время) к необходимой им информации;
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
- защиты части информации от незаконного её тиражирования (защиты авторских прав, прав собственника информации и т.п.).

4.2 Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений (интересы которых затрагиваются при создании и функционировании АС) от возможного нанесения им ощутимого материального, физического, морального или иного ущерба посредством случайного или пред-

намеренного несанкционированного вмешательства в процесс функционирования АС или несанкционированного доступа к циркулирующей в ней информации и её незаконного использования.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации и системы её обработки:

- доступности обрабатываемой информации для зарегистрированных пользователей (устойчивого функционирования АС, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время);
- сохранения в тайне (обеспечения конфиденциальности) определенной части информации, хранимой, обрабатываемой средствами вычислительной техники (СВТ) и передаваемой по каналам связи;
- целостности и достоверности информации, хранимой и обрабатываемой в АС и передаваемой по каналам связи.

4.3 Основные задачи системы обеспечения информационной безопасности АС

Для достижения основной цели защиты и обеспечения указанных свойств информации и системы её обработки система безопасности АС должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования АС посторонних лиц (возможность использования автоматизированной системы и доступ к её ресурсам должны иметь только зарегистрированные установленным порядком пользователи – работники структурных подразделений Общества);
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам АС (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям АС для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:
- к информации, циркулирующей в АС;
- средствам вычислительной техники (СВТ) АС;
- аппаратным, программным и криптографическим средствам защиты, используемым в АС;
- регистрацию действий пользователей при использовании защищаемых ресурсов АС в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов ответственными за информационную безопасность;
- контроль целостности (обеспечение неизменности) среды исполнения программ и её восстановление в случае нарушения;
- защиту от несанкционированной модификации и контроль целостности используемых в АС программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации ограниченного распространения от утечки по техническим каналам при её обработке, хранении и передаче по каналам связи;
- защиту информации ограниченного распространения, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

- своевременное выявление источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности.

4.4 Основные пути достижения целей защиты (решения задач системы защиты)

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учетом всех подлежащих защите ресурсов системы (информации, систем управления базами данных и другого системного и прикладного программного обеспечения, каналов связи, серверов, АРМ);
- регламентацией процессов обработки подлежащей защите информации, с применением средств автоматизации и действий работников структурных подразделений Общества, использующих АС, а также действий персонала, осуществляющего обслуживание и модификацию программных и технических средств АС, на основе утвержденных генеральным директором Общества организационно-распорядительных документов по вопросам обеспечения информационной безопасности;
- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Общества по вопросам обеспечения информационной безопасности;
- назначением и подготовкой должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности и процессов её обработки;
- наделением каждого пользователя АС минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к ресурсам АС;
- четким знанием и строгим соблюдением всеми работниками, использующими и обслуживающими аппаратные и программные средства АС, требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;
- персональной ответственностью за свои действия каждого работника, участвующего в рамках своих функциональных обязанностей, в процессах автоматизированной обработки информации и имеющего доступ к ресурсам АС;
- реализацией технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения, технических средств и данных;
- принятием эффективных мер обеспечения физической целостности технических средств и непрерывным поддержанием необходимого уровня защищенности компонентов АС;
- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
- разграничением потоков информации различного уровня конфиденциальности, а также запрещением передачи информации ограниченного распространения по незащищенным каналам связи;
- эффективным контролем соблюдения работниками подразделений Общества – пользователями АС требований по обеспечению информационной безопасности;
- юридической защитой интересов Общества при взаимодействии его подразделений с внешними организациями (связанном с обменом информацией) от противоправных дей-

ствий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц;

- проведением постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработкой и реализацией предложений по совершенствованию системы защиты информации в АС.

5. Основные угрозы информационной безопасности АС

5.1 Угрозы информационной безопасности и их источники

Наиболее опасными (значимыми) угрозами информационной безопасности АС (способами нанесения ущерба субъектам информационных отношений) являются:

- нарушение конфиденциальности (разглашение, утечка) сведений, составляющих коммерческую или врачебную тайну, а также персональных данных;
- нарушение работоспособности (дезорганизация работы) АС, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;
- нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов АС, а также фальсификация (подделка) документов.

Основными источниками угроз информационной безопасности АС являются:

- непреднамеренные (ошибочные, случайные, необдуманные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований информационной безопасности и другие действия работников (в том числе администраторов средств защиты) структурных подразделений Общества при эксплуатации АС, приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности отдельных рабочих станций (АРМ), подсистем или АС в целом;
- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия работников подразделений Общества, допущенных к работе с АС, а также работников подразделений Общества, отвечающих за обслуживание, администрирование программного и аппаратного обеспечения, средств защиты и обеспечения информационной безопасности;
- воздействия из других логических и физических сегментов АС со стороны работников других подразделений Общества, в том числе программистов-разработчиков прикладных задач, а также удаленное несанкционированное вмешательство посторонних лиц из телекоммуникационных сетей Общества и внешних сетей общего назначения (Internet) через легальные и несанкционированные каналы подключения сети Общества к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам АС;
- деятельность международных и отечественных преступных групп и формирований, политических и экономических структур, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности системы в целом и её отдельных компонентов;
- ошибки, допущенные при проектировании АС и её системы защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты) АС;
- аварии, стихийные бедствия и т.п.

5.2 Пути реализации непреднамеренных искусственных (субъективных) угроз информационной безопасности в АС

Пользователи, операторы, системные администраторы и работники Общества, обслуживающие систему, являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций и процедур.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз АС (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла) и меры по нейтрализации соответствующих угроз и снижению возможного наносимого ими ущерба приведены в Таблице 5.1.

Таблица 5.1.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз АС	Меры по нейтрализации угроз и снижению возможного наносимого ущерба
Действия работников Общества, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств; отключению оборудования или изменение режимов работы устройств и программ; разрушению информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение программ или файлов с важной информацией, в том числе системных, повреждение каналов связи, неумышленная порча носителей информации и т.п.)	1. Организационные меры (регламентация действий, введение запретов). 2. Применение физических средств, препятствующих неумышленному совершению нарушения. 3. Применение технических (аппаратно-программных) средств разграничения доступа к ресурсам. 4. Резервирование критичных ресурсов.
Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.)	1. Организационные меры (удаление всех потенциально опасных программ с дисков ПЭВМ АРМ). 2. Применение технических (аппаратно-программных) средств разграничения доступа к технологическим и инструментальным программам на дисках ПЭВМ АРМ.
Несанкционированное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения работниками своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (процессорного времени, оперативной памяти, памяти на внешних носителях и т.п.)	1. Организационные меры (введение запретов). 2. Применение технических (аппаратно-программных) средств, препятствующих несанкционированному внедрению и использованию неучтенных программ.
Непреднамеренное заражение компьютера вирусами	1. Организационные меры (регламентация действий, введение запретов). 2. Технологические меры (применение специальных программ обнаружения и уничтожения вирусов). 3. Применение аппаратно-программных средств, препятствующих заражению компьютеров компьютерными вирусами.
Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования или ЭЦП, идентификационных карточек, пропусков и т.п.)	1. Организационные меры (регламентация действий, введение запретов, усиление ответственности). 2. Применение физических средств обеспечения сохранности указанных реквизитов.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз АС	Меры по нейтрализации угроз и снижению возможного наносимого ущерба
Игнорирование организационных ограничений (установленных правил) при работе в системе	1. Организационные меры (усиление ответственности и контроля). 2. Использование дополнительных физических и технических средств защиты.
Некомпетентное использование, настройка или неправомерное отключение средств защиты ответственными за информационную безопасность	1. Организационные меры (обучение персонала, усиление ответственности и контроля).
Ввод ошибочных данных	1. Организационные меры (усиление ответственности и контроля). 2. Технологические меры контроля ошибок операторов ввода данных.

5.3 Умышленные действия сторонних лиц, зарегистрированных пользователей и обслуживающего персонала

Возможные основные пути умышленной дезорганизации работы, вывода АС из строя, проникновения в систему и несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.) и меры по нейтрализации соответствующих угроз и снижению возможного наносимого ими ущерба приведены в Таблице 5.2.

Таблица 5.2

Основные возможные пути умышленной дезорганизации работы, вывода АС из строя, проникновения в систему и НСД к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.)	Меры по нейтрализации угроз и снижению возможного наносимого ущерба
Физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов автоматизированной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.), отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, линий связи и т.п.)	1. Организационные меры (регламентация действий, введение запретов). 2. Применение физических средств, препятствующих неумышленному совершению нарушения. 3. Резервирование критичных ресурсов. 4. Обеспечение личной безопасности работников.
Внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность), вербовка (путем подкупа, шантажа, угроз и т.п.) пользователей, имеющих определенные полномочия по доступу к защищаемым ресурсам	1. Организационные меры (подбор, расстановка и работа с персоналом, усиление контроля и ответственности). 2. Автоматическая регистрация действий персонала.
Хищение носителей информации (распечаток, магнитных дисков, лент, микросхем памяти, запоминающих устройств и ПЭВМ), хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.)	1. Организационные меры (организация хранения и использования носителей с защищаемой информацией).
Несанкционированное копирование носителей информации, чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств	1. Организационные меры (организация хранения и использования носителей с защищаемой информацией). 2. Применение технических средств разграничения доступа к защищаемым ресурсам 3. Регистрация получения твердых копий документов с наиболее критичной информацией.

Основные возможные пути умышленной дезорганизации работы, вывода АС из строя, проникновения в систему и НСД к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.)	Меры по нейтрализации угроз и снижению возможного наносимого ущерба
Несанкционированное копирование конфиденциальной информации на внешние носители информации или передача её при помощи средств телекоммуникаций (электронная почта, Internet, модемы и т.п.)	1. Организационные меры (регламентация действий, введение запретов, работа с персоналом). 2. Применение программно-аппаратных средств, ограничивающих использование внешних носителей информации. 3. Регистрация и анализ использования средств телекоммуникаций, оперативное реагирование на несанкционированные действия.
Незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы программными закладками и т.д.) с последующей маскировкой под зарегистрированного пользователя.	1. Организационные меры (регламентация действий, введение запретов, работа с персоналом). 2. Применение технических средств, препятствующих внедрению программ перехвата паролей, ключей и других реквизитов.
Несанкционированное использование АРМ пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.	1. Организационные меры (строгая регламентация доступа в помещения и допуска к работам на данных АРМ). 2. Применение физических и технических средств разграничения доступа.
Несанкционированная модификация программного обеспечения – внедрение программных «закладок», «троянских коней» и «жучков», то есть вредоносного кода, который не нужен для осуществления заявленных функций, но позволяет преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи защищаемой информации или дезорганизации функционирования системы.	1. Организационные меры (строгая регламентация допуска к работам). 2. Применение физических и технических средств разграничения доступа и препятствующих несанкционированной модификации аппаратно-программной конфигурации АРМ. 3. Применение средств контроля целостности программ.
Перехват данных, передаваемых по каналам связи, и их анализ с целью получения конфиденциальной информации и выяснения протоколов обмена, правил вхождения в связь и авторизации пользователей и последующих попыток их имитации для проникновения в систему	1. Физическая защита каналов связи. 2. Применение средств криптографической защиты (шифрования) передаваемой информации.
Вмешательство в процесс функционирования АС сетей общего пользования с целью несанкционированной модификации данных, доступа к конфиденциальной информации, дезорганизации работы подсистем и т.п.	1. Организационные меры (регламентация подключения и работы в сетях общего пользования). 2. Применение специальных технических средств защиты (межсетевых экранов, средств контроля защищенности и обнаружения атак на ресурсы системы и т.п.).

5.4 Утечка информации по техническим каналам

При проведении мероприятий и эксплуатации технических средств возможны следующие каналы утечки или нарушения целостности информации, нарушения работоспособности технических средств:

- побочные электромагнитные излучения информативного сигнала от технических средств АС и линий передачи информации;
- наводки информативного сигнала, обрабатываемого АС, на провода и линии, выходящие

за пределы контролируемой зоны Общества, в т.ч. на цепи заземления и электропитания;

- электрические сигналы или радиоизлучения, обусловленные воздействием на АС высокочастотных сигналов, создаваемых с помощью разведывательной аппаратуры, по эфиру и проводам, либо сигналов промышленных радиотехнических устройств (радиовещательные, радиолокационные станции, средства радиосвязи и т.п.), и модуляцией их информативным сигналом (облучение, «навязывание»);
- радиоизлучения или электрические сигналы от внедренных в АС и выделенные помещения специальных электронных устройств перехвата информации («закладок»), модулированные информативным сигналом;
- радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;
- акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации (принтер, пишущая машинка и т.п.);
- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации;
- вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации выделенных помещений;
- просмотр информации с экранов мониторов и других средств её отображения с помощью оптических средств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена, в том числе электромагнитное, через специально внедренные электронные и программные средства.

Перехват информации ограниченного распространения или воздействие на нее с использованием технических средств может вестись из зданий, расположенных в непосредственной близости от объектов информатизации, мест временного пребывания заинтересованных в перехвате информации или воздействии на нее лиц при посещении ими подразделений Общества, а также с помощью скрытно устанавливаемой автономной автоматической аппаратуры на прилегающих территориях.

В качестве аппаратуры разведки или воздействия на информацию и технические средства могут использоваться:

- космические средства разведки для перехвата радиоизлучений от средств радиосвязи, радиорелейных станций, и приема сигнала от автономных автоматических средств разведки и электронных устройств перехвата информации;
- стационарные средства, размещаемые в зданиях;
- портативные возимые и носимые средства, размещаемые в зданиях, в транспортных средствах, а также носимые лицами, ведущими разведку;
- автономные автоматические средства, скрытно устанавливаемые на объектах защиты или поблизости от них.

Стационарные средства обладают наибольшими энергетическими, техническими и функциональными возможностями. В то же время они, как правило, удалены от объектов защиты и не имеют возможности подключения к линиям, коммуникациям и сооружениям. Портативные средства могут использоваться непосредственно на объектах защиты или поблизости от них и могут подключаться к линиям и коммуникациям, выходящим за пределы

контролируемой территории.

Кроме перехвата информации техническими средствами разведки возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны. Такого рода утечка информации возможна вследствие:

- непреднамеренного прослушивания без использования технических средств разговоров, ведущихся в выделенном помещении, из-за недостаточной звукоизоляции его ограждающих конструкций, систем вентиляции и кондиционирования воздуха;
- случайного прослушивания телефонных переговоров при проведении профилактических работ на АТС, кроссах, кабельных коммуникациях с помощью контрольной аппаратуры;
- просмотра информации с экранов мониторов и других средств её отображения.

5.5 Неформальная модель возможных нарушителей

НАРУШИТЕЛЬ — это лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Система защиты АС должна строиться исходя из предположений о следующих возможных типах нарушителей в системе (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

«Неопытный (невнимательный) пользователь» — работник Общества (или другой организации, зарегистрированный как пользователь системы), который может предпринимать попытки выполнения запрещенных операций, доступа к защищаемым ресурсам АС с превышением своих полномочий, ввода некорректных данных и т.п. действия по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (доступные ему) аппаратные и программные средства.

«Любитель» — работник Общества (или другой организации, зарегистрированный как пользователь системы), пытающийся преодолеть систему защиты без корыстных целей и злого умысла, для самоутверждения или из «спортивного интереса». Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам (имен, паролей и т.п. других пользователей), недостатки в построении системы защиты и доступные ему штатные (установленные на рабочей станции) программы (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства (отладчики, служебные утилиты), самостоятельно разработанные программы или стандартные дополнительные технические средства.

«Мошенник» — работник Общества (или другой организации, зарегистрированный как пользователь системы), который может предпринимать попытки выполнения незаконных технологических операций, ввода подложных данных и тому подобные действия в корыстных целях, по принуждению или из злого умысла, но использующий при этом только штатные (установленные на рабочей станции и доступные ему) аппаратные и программные средства от своего имени или от имени другого работника (зная его имя и пароль, используя его кратковременное отсутствие на рабочем месте и т.п.).

«Внутренний злоумышленник» — работник Общества, зарегистрированный как пользователь системы, действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно, в сговоре с лицами, не являющимися работниками Общества. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы получения реквизитов доступа, пассивные средства (технические средства перехвата без модификации компонентов системы), методы и средства активного воздей-

ствия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий как изнутри, так и извне – из сетей общего пользования.

Внутренним нарушителем может быть лицо из следующих категорий персонала Общества:

- зарегистрированные конечные пользователи АС (работники Общества);
- работники, не допущенные к работе с АС;
- персонал, обслуживающий технические средства АС (инженеры, техники);
- работники подразделений разработки и сопровождения ПО (прикладные и системные программисты);
- технический персонал, обслуживающий здания (уборщицы, электрики, сантехники и другие работники, имеющие доступ в здания и помещения, где расположены компоненты АС);
- работники и подразделения информационной безопасности;
- руководители различных уровней.

«Внешний нарушитель (злоумышленник)» — постороннее лицо или работник Общества (или другой организации, зарегистрированный как пользователь системы), действующий целенаправленно из корыстных интересов, из мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор радиоэлектронных способов нарушения информационной безопасности, методов и средств взлома систем защиты, характерных для сетей общего пользования (в особенности сетей на основе IP-протокола), включая удаленное внедрение программных закладок и использование специальных инструментальных и технологических программ, используя имеющиеся слабости протоколов обмена и системы защиты узлов сети АС.

Категории лиц, которые могут быть *внешними нарушителями*:

- уволенные работники Общества;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);
- посетители (приглашенные представители организаций, граждане), представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.;
- члены преступных организаций, работники спецслужб или лица, действующие по их заданию;
- лица, случайно или умышленно проникшие в сети АС из внешних (по отношению к Обществу) сетей телекоммуникации («хакеры»).

Пользователи и обслуживающий персонал из числа работников Общества имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих правил и инструкций. Особую опасность эта группа нарушителей представляет при взаимодействии с криминальными структурами или спецслужбами.

Уволенные работники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. Полученные в Обществе знания и опыт выделяют их среди других источников внешних угроз.

Криминальные структуры представляют наиболее агрессивный источник внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность работников Общества всеми доступными им силами

и средствами.

Профессиональные «хакеры» имеют наиболее высокую техническую квалификацию и знания об уязвимостях программных средств, используемых в АС. Наибольшую угрозу представляют при взаимодействии с работающими и уволенными работниками Общества и криминальными структурами.

Организации, занимающиеся разработкой, поставкой и ремонтом оборудования, информационных систем, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам. Криминальные структуры и спецслужбы могут использовать эти организации для временного устройства на работу своих членов, с целью доступа к защищаемой информации в АС.

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

- работа по подбору персонала и специальные мероприятия исключают возможность создания сообществ нарушителей, т.е. объединения (сговора) и целенаправленных действий двух и более нарушителей – работников Общества по преодолению системы защиты;
- нарушитель скрывает свои несанкционированные действия от других работников Общества;
- несанкционированные действия могут быть следствием ошибок пользователей, администраторов безопасности, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
- в своей противоправной деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей.

6. Основные положения технической политики в области обеспечения информационной безопасности АС

6.1 Техническая политика в области обеспечения информационной безопасности

Реализация технической политики в области обеспечения информационной безопасности должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищенности информации не только с помощью одного отдельного средства (мероприятия), но и с помощью их простой совокупности. Необходимо их взаимное согласование между собой (комплексное применение), а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищенном исполнении при оптимальном соотношении технических (аппаратных, программных) средств и организационных мероприятий.

Основными направлениями реализации технической политики обеспечения информационной безопасности АС являются:

- обеспечение защиты информационных ресурсов от хищения, утраты, утечки, уничтожения, искажения или подделки за счет несанкционированного доступа и специальных воздействий (от НСД);
- обеспечение защиты информации от утечки по техническим каналам при её обработке, хранении и при передаче по каналам связи.

Система обеспечения информационной безопасности АС должна предусматривать комплекс организационных, программных и технических средств и мер по защите информации в процессе её обработки и хранения, при передаче информации по каналам связи, при ведении конфиденциальных переговоров, раскрывающих сведения с ограниченным досту-

пом, при использовании импортных технических и программных средств.

В рамках указанных направлений технической политики обеспечения информационной безопасности осуществляются:

- реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к работам, документам и информации конфиденциального характера;
- реализация системы инженерно-технических и организационных мер охраны, предусматривающей многорубежность и равнопрочность построения охраны (территории, здания, помещения) с комплексным применением современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;
- ограничение доступа исполнителей и посторонних лиц в здания и помещения, где проводятся работы конфиденциального характера и размещены средства информатизации и коммуникации, на которых обрабатывается (хранится, передается) информация конфиденциального характера, непосредственно к самим средствам информатизации и коммуникациям;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации в подсистемах различного уровня и назначения, входящих в АС;
- учет документов, информационных массивов, регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступы и действий пользователей, обслуживающего персонала и посторонних лиц;
- предотвращение внедрения в автоматизированные подсистемы программ-вирусов, программных закладок и т.п.
- криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;
- надежное хранение традиционных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее хищение, подмену и уничтожение;
- необходимое резервирование технических средств и дублирование массивов и носителей информации;
- снижение уровня и информативности побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых различными элементами автоматизированных подсистем;
- обеспечение акустической защиты помещений, в которых обсуждается информация конфиденциального характера;
- электрическая развязка цепей питания, заземления и других цепей объектов информатизации, выходящих за пределы контролируемой зоны;
- активное зашумление в различных диапазонах;
- противодействие оптическим и лазерным средствам наблюдения.

6.2 Формирование режима информационной безопасности

С учетом выявленных угроз информационной безопасности АС режим защиты должен формироваться как совокупность способов и мер защиты циркулирующей в автоматизированной системе информации и поддерживающей её инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, влекущих за собой нанесение ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

Комплекс мер по формированию режима информационной безопасности включает:

- установление в Обществе организационно-правового режима информационной безопасности (нормативные документы, работа с персоналом, делопроизводство);

- выполнение организационно-технических мероприятий по защите информации ограниченного распространения от утечки по техническим каналам;
- организационные и программно-технические мероприятия по предупреждению несанкционированных действий (доступа) к информационным ресурсам АС;
- комплекс мероприятий по контролю функционирования средств и систем защиты информационных ресурсов ограниченного распространения после случайных или преднамеренных воздействий;
- комплекс оперативных мероприятий подразделений безопасности по предотвращению (выявлению) проникновения в Общества информаторов, связанных с преступными сообществами.

Организационно-правовой режим предусматривает создание и поддержание правовой базы информационной безопасности, а также разработку (введение в действие) следующих организационно-распорядительных документов:

- Положение о защите конфиденциальной информации. Указанное Положение регламентирует организацию, порядок работы со сведениями ограниченного распространения, обязанности и ответственность работников, допущенных к этим сведениям, порядок передачи материалов, содержащих сведения ограниченного распространения, государственным и коммерческим учреждениям и организациям;
- Перечень сведений, содержащих конфиденциальную информацию. Перечень определяет сведения, отнесенные к категориям конфиденциальных (государственная, коммерческая, врачебная тайна, персональные данные и др.), уровень и сроки действия ограничений по доступу к защищаемой информации;
- Приказы и распоряжения по установлению режима информационной безопасности:
- о допуске работников к работе с информацией ограниченного распространения;
- о назначении лиц ответственных за обеспечение сохранности информации ограниченного распространения в АС и др.;
- Нормативно-распорядительные документы Общества:
- по организации охранно-пропускного режима;
- по организации делопроизводства;
- по организации работы с информацией на отчуждаемых носителях;
- о защите конфиденциальной информации в АС;
- по изменению конфигурации программного и аппаратного обеспечения;
- другие нормативные документы.

Организационно-технические мероприятия по защите конфиденциальной информации от утечки по техническим каналам предусматривают:

- комплекс мер и соответствующих технических средств, ослабляющих утечку информации — пассивная защита (защита);
- комплекс мер и соответствующих технических средств, создающих помехи при съеме информации — активная защита (противодействие);
- комплекс мер и соответствующих технических средств, позволяющих выявлять каналы утечки информации — поиск (обнаружение).

Физическая охрана объектов информатизации (компонентов компьютерных систем) включает:

- организацию системы охранно-пропускного режима и системы контроля допуска на объект;
- введение дополнительных ограничений по доступу в помещения, предназначенные для хранения закрытой информации (кодовые и электронные замки, карточки допуска и т.д.);

- визуальный и технический контроль контролируемой зоны объектов защиты;
- применение систем охранной и пожарной сигнализации и т.д.

Выполнение режимных требований при работе с информацией ограниченного распространения предполагает:

- разграничение допуска к информационным ресурсам ограниченного распространения;
- разграничение допуска к программно-аппаратным ресурсам АС;
- ведение учета ознакомления работников с конфиденциальной информацией;
- включение в функциональные обязанности работников обязательства о неразглашении и сохранности конфиденциальных сведений;
- исключение возможности копирования конфиденциальной информации на отчуждаемые носители информации и передачи её при помощи средств телекоммуникаций (электронная почта, Internet, модемы и т.п.)
- организация уничтожения информационных отходов (бумажных, магнитных и т.д.);
- оборудование служебных помещений сейфами, шкафами для хранения бумажных и магнитных носителей информации и т.д.

Мероприятия технического контроля предусматривают:

- контроль проведения технического обслуживания, ремонта носителей информации и средств вычислительной техники;
- проверки поступающего оборудования, предназначенного для обработки закрытой информации, на наличие специально внедренных устройств;
- инструментальный контроль технических средств на наличие побочных электромагнитные излучения и наводок;
- оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи;
- постоянное обновление технических и программных средств защиты от несанкционированного доступа к информации в соответствие с меняющейся оперативной обстановкой.

6.3 Оснащение техническими средствами хранения и обработки информации

Организация хранения конфиденциальных документов и машинных носителей информации, а также оборудование режимных помещений осуществляется в соответствии с установленными в Обществе требованиями.

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании инструкции, утверждаемой генеральным директором Общества или директорами филиалов после согласования с подразделениями безопасности соответствующих объектов охраны.

На случай пожара, аварии или стихийного бедствия подразделениями безопасности разрабатывается инструкция, утверждаемая генеральным директором Общества, в которой предусматривается порядок вызова должностных лиц, вскрытия режимных помещений, очередность и порядок спасения секретных документов и изделий и дальнейшего их хранения. Инструкция должна находиться в подразделении охраны, независимо от его ведомственной принадлежности.

Подразделения Общества должны быть обеспечены средствами уничтожения документов.

Работы по обеспечению информационной безопасности, обрабатываемой с помощью АС, можно условно разделить на следующие группы:

- обеспечение физической безопасности компонентов АС (защита от специально внедренных закладных устройств, повреждений, сбоев питания, краж и т.п.);
- обеспечение логической безопасности АС (защита от несанкционированного доступа, от ошибок в действиях пользователей и программ и т.д.);
- обеспечение социальной безопасности АС (разработка организационных документов, соответствующих законодательным нормам, регулирующих применение компьютерных технологий, порядок расследования и наказания за компьютерные преступления, контроль и предотвращение неправильного использования информации в случае, когда она хранится или обрабатывается с помощью компьютерных систем).

7. Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения информационной безопасности АС и её функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- разумная достаточность;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

Законность

Предполагает осуществление защитных мероприятий и разработку системы информационной безопасности АС в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», другим нормативным актам по информационной безопасности, утвержденным органами государственной власти и управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Принятые меры информационной безопасности не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях к информации конкретных систем.

Пользователи и обслуживающий персонал АС должны иметь представление об ответственности за правонарушения в области систем автоматизированной обработки информации (статьи 272, 273, 274 и 293 Уголовного Кодекса РФ, статьи 13.11 и 13.12 Кодекса РФ об административных правонарушениях и др.).

Системность

Системный подход к построению системы защиты информации в АС предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов,

условий и факторов, существенно значимых для понимания и решения проблемы обеспечения информационной безопасности АС.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных её компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства защиты, реализованные на уровне операционных систем (ОС) СВТ в силу того, что ОС – это та часть компьютерной системы, которая управляет использованием всех её ресурсов. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

Непрерывность защиты

Защита информации – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС, начиная с самых ранних стадий проектирования, а не только на этапе её эксплуатации.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления её функционирования.

Своевременность

Предполагает упреждающий характер мер обеспечения информационной безопасности, то есть постановку задач по комплексной защите АС и реализацию мер обеспечения информационной безопасности на ранних стадиях разработки АС в целом и её системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования АС и её системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

Разумная достаточность
(экономическая целесообразность, сопоставимость возможного ущерба и затрат)

Предполагает соответствие уровня затрат на обеспечение информационной безопасности ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы АС, в которой эта информация циркулирует. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств можно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов компьютерной системы и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа рисков).

Персональная ответственность

Предполагает возложение ответственности за обеспечение информационной безопасности и системы её обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

Принцип минимизации полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах подразделений Общества. В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

Гибкость системы защиты

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса её нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости системы защиты избавляет владельцев АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования её подсистем. Знание алгоритмов работы системы защиты не должно давать возможности её преодоления (даже авторами). Это, однако, не означает, что информация о конкретной системе защиты должна быть общедоступна.

Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня информационной безопасности и должны соответствовать установленным нормам и требованиям информационной безопасности.

Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области (Федеральный закон от 08.08.2001 № 128-ФЗ «О лицензировании отдельных видов деятельности»). Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Общества (специалистами по информационной безопасности).

Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил информационной безопасности на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль деятельности любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

8. Меры, методы и средства обеспечения требуемого уровня защищённости информационных ресурсов

8.1 Меры обеспечения безопасности

Все меры обеспечения безопасности АС подразделяются на:

- правовые (законодательные);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

8.1.1 Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в РФ законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе её обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым

неправомерному использованию информации, и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

8.1.2 Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения компьютеров и сети Internet в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неформальные (например, общепризнанные нормы честности и т.п.), так и формальные, то есть оформленные в некоторый свод правил (устав) или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

8.1.3 Организационные (административные) меры защиты

Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Формирование политики безопасности

Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать политику в области обеспечения информационной безопасности (отражающую подходы к защите информации) и обеспечить её выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения информационной безопасности в АС целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность Общества в целом. Примером таких решений являются:

- принятие решения о формировании комплексной программы обеспечения информационной безопасности, определение ответственных за её реализацию;
- формулирование целей, постановка задач, определение направлений деятельности в области информационной безопасности;
- принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне Общества в целом;
- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна четко определить область влияния и ограничения при определении целей информационной безопасности; определить, какими ресурсами (материальные, персонал) они будут достигнуты; и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью АС.

Политика нижнего уровня определяет процедуры и правила достижения целей и решения задач информационной безопасности и детализирует (регламентирует) эти правила:

- какова область применения политики информационной безопасности;
- каковы роли и обязанности должностных лиц, отвечающие за проведение политики информационной безопасности;
- кто имеет права доступа к информации ограниченного распространения;

- кто и при каких условиях может читать и модифицировать информацию и т.д.

Политика нижнего уровня:

- регламентирует информационные отношения, исключающие возможность произвольных, монопольных или несанкционированных действий в отношении конфиденциальных информационных ресурсов;
- определяет групповые и иерархические принципы и методы разделения секретов и разграничения доступа к информации ограниченного распространения;
- определяет программно-математические и технические (аппаратные) средства криптозащиты, противодействия НСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

Регламентация доступа в помещения АС

Эксплуатация защищенных серверов АС должна осуществляться в помещениях, оборудованных автоматическими замками, средствами сигнализации, исключающих возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающих физическую сохранность находящихся в помещении защищаемых ресурсов (серверов, документов, реквизитов доступа и т.п.). Размещение и установка технических средств таких серверов должна исключать возможность визуального просмотра вводимой (выводимой) информации лицами, не имеющими к ней отношения. Уборка помещений должна производиться с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

В помещениях во время обработки и отображения на ПЭВМ информации ограниченного распространения должен присутствовать только персонал, допущенный к работе с данной информацией. Запрещается прием посетителей в помещениях, когда осуществляется обработка защищаемой информации.

Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами и металлическими шкафами.

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции, утверждаемой руководством Общества.

Регламентация допуска работников к использованию ресурсов АС

В рамках разрешительной системы допуска устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях; система разграничения доступа, которая предполагает определение для всех пользователей автоматизированной информационной системы информационных и программных ресурсов, доступных им для конкретных операций (чтение, запись, модификация, удаление, выполнение) с помощью заданных программно-технических средств доступа.

Допуск работников подразделений Общества к работе с автоматизированной системой и доступ к её ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем АС должны производиться установленным порядком согласно «Положению о распределении доступа пользователей к проведению операций в программном обеспечении, а также к базам данных в компьютерных системах Общества». Основными пользователями информации в АС являются работники структурных подразделений Общества. Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

- открытая и конфиденциальная информация размещаются по возможности на различных серверах (это упрощает обеспечение защиты) или различных ресурсах одного сервера;
- каждый работник пользуется только предписанными ему правами по отношению к ин-

формации, с которой ему необходима работа в соответствии с должностными обязанностями;

- руководитель имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями;
- наиболее ответственные технологические операции должны производиться по принципу разделения ответственности, т.е. правильность введенной информации подтверждается другим должностным лицом (работником), не имеющим права ввода информации.

Все работники Общества, допущенные к работе (пользователи) и обслуживающий персонал АС, должны нести персональную ответственность за нарушения установленного порядка автоматизированной обработки информации, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов АС. Каждый работник (при приеме на работу) должен подписывать «Договор о неразглашении конфиденциальной информации», а также ознакомиться с «Инструкцией о порядке работы с конфиденциальной информацией в АС».

Обработка защищаемой информации в подсистемах АС должна производиться в соответствии с утвержденными технологическими инструкциями (регламентами, процедурами и пр.) для данных подсистем.

Для пользователей защищенных АРМ (то есть АРМ, на которых обрабатывается конфиденциальная информация или решаются подлежащие защите задачи и на которых установлены соответствующие средства защиты) должны быть разработаны необходимые технологические инструкции, включающие требования по обеспечению информационной безопасности.

Регламентация процессов ведения баз данных и осуществления модификации информационных ресурсов

Все операции по ведению баз данных Общества и допуск работников подразделений Общества к работе с этими базами данных строго регламентируются (производятся в соответствии с утвержденными технологическими инструкциями). Любые изменения состава и полномочий пользователей баз данных АС производятся в установленном порядке.

Распределение имен, генерация паролей, сопровождение правил разграничения доступа к базам данных возлагается на специальных пользователей – администраторов соответствующих баз данных. При этом могут использоваться как штатные, так и дополнительные средства защиты СУБД и операционных систем.

Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов АС

Все рабочие места, серверы и программные ресурсы АС должны быть установленным порядком категорированы (для каждого ресурса должен быть определен требуемый уровень защищенности). Подлежащие защите ресурсы системы (программы, АРМ) подлежат строгому учету (на основе использования соответствующих формуляров или специализированных баз данных).

Аппаратно-программная конфигурация автоматизированных рабочих мест, на которых обрабатывается конфиденциальная информация (с которых возможен доступ к защищаемым ресурсам), должна соответствовать кругу возложенных на пользователей данного АРМ функциональных обязанностей. Все неразрешенные для использования в работе устройства ввода-вывода информации (USB-, COM-, LPT-порты, НГМД, CD, DVD- дисководы, устройства Flash-памяти и другие носители информации) на таких АРМ должны быть отключены (удалены) или заблокированы, не нужные для работы программные средства и данные с дисков АРМ также должны быть удалены. Порядок подключения устройств ввода-вывода на таких АРМ должен быть регламентирован.

Для упрощения сопровождения, обслуживания и организации защиты АРМ должны

оснащаться программными средствами и конфигурироваться унифицировано (в соответствии с установленными правилами).

Должны быть предусмотрены механизмы, исключающие несанкционированное изменение конфигурации аппаратных средств, установленных на рабочих местах пользователей.

Ввод в эксплуатацию новых АРМ и все изменения в конфигурации технических и программных средств существующих АРМ в АС должны осуществляться только установленным порядком.

Все программное обеспечение (разработанное специалистами Общества, полученное централизованно или приобретенной у фирм-производителей) должно установленным порядком проходить испытания и передаваться в библиотеку эталонного программного обеспечения (БЭПО) Общества. В подсистемах АС должны устанавливаться и использоваться только полученные установленным порядком из БЭПО программные средства. Использование в АС ПО, не учтенного в БЭПО, должно быть запрещено.

Разработка ПО задач, проведение испытаний разработанного и приобретенного ПО, передача ПО в эксплуатацию должна осуществляться в соответствии с установленным порядком разработки, проведения испытаний и передачи задач в эксплуатацию.

Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов АС

На всех АРМ, подлежащих защите, должны быть установлены необходимые технические средства защиты (соответствующие категории данных, обрабатываемых данным АРМ).

Кадровая работа (подбор и подготовка персонала, обучение пользователей)

До начала этапа эксплуатации автоматизированной системы её пользователи, а также необходимый руководящий и обслуживающий персонал должны быть ознакомлены с перечнем сведений, подлежащих защите, в части их касающейся, и своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации ограниченного распространения.

Защита информации по всем перечисленным направлениям возможна только после выработки у пользователей определенной дисциплины, т.е. норм, обязательных для исполнения всеми, кто работает с АС. К таким нормам относятся запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу АС, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей.

Все работники Общества, использующие при работе конкретные подсистемы АС, должны быть ознакомлены с организационно-распорядительными документами по защите АС в части, их касающейся, должны знать и неукоснительно выполнять технологические инструкции и общие обязанности по обеспечению информационной безопасности при использовании АС. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, должно осуществляться руководителями подразделений под личную подпись.

Подразделения, отвечающие за реализацию политики информационной безопасности

За непосредственную организацию (построение) и эффективное функционирование системы защиты информации АС отвечают подразделения информационного обеспечения и директора соответствующих филиалов.

На них возлагается решение следующих основных задач:

- проведение в жизнь политики информационной безопасности, определение требований к системе защиты информации;

- организация мероприятий и координация работ всех подразделений Общества по комплексной защите информации;

Основные функции подразделений информационного обеспечения при реализации политики заключаются в следующем:

- формирование требований к системе защиты в процессе создания (развития) АС;
- участие в проектировании системы защиты, её испытаниях и приемке в эксплуатацию;
- планирование, организация и обеспечение функционирования системы защиты информации в процессе функционирования АС;
- распределение между пользователями необходимых реквизитов защиты;
- наблюдение за функционированием системы защиты и её элементов;
- обучение пользователей и персонала АС правилам безопасной обработки информации;
- регламентация действий и контроль администраторов баз данных, серверов и сетевых устройств (за работниками, обеспечивающими правильность применения имеющихся в составе ОС, СУБД и т.п. средств разграничения доступа и других средств защиты информации);
- контроль соблюдения пользователями и персоналом АС установленных правил обращения с конфиденциальной информацией в процессе её автоматизированной обработки, передачи и хранения;
- принятие мер при попытках НСД к информации и при нарушениях правил функционирования системы защиты.

В подразделениях информационного обеспечения должны быть выделены специальные работники для выполнения всех перечисленных выше функций. В целях исключения конфликта интересов они не должны иметь других обязанностей, связанных с функционированием АС.

Контроль реализации политики безопасности и оценку эффективности принятых мер и применяемых средств защиты информации осуществляют администраторы информационной безопасности. Их функции заключаются в следующем:

- организация проверок надежности функционирования системы защиты;
- оценка эффективности системы контроля баз данных, серверов и сетевых устройств (за работниками, обеспечивающими правильность применения имеющихся в составе ОС, СУБД и т.п. средств разграничения доступа и других средств защиты информации);
- оценка системы контроля соблюдения пользователями и персоналом АС установленных правил обращения с конфиденциальной информацией;
- организация проверок соблюдения пользователями и персоналом АС установленных правил обращения с конфиденциальной информацией; расследование инцидентов, связанных с нарушениями правил обращения с конфиденциальной информацией.

Администраторам информационной безопасности, на которых возложено выполнение перечисленных выше функций, должны обеспечиваться все условия, необходимые для выполнения этих функций. Они должны иметь права:

- определять необходимость разработки нормативных документов, касающихся вопросов обеспечения информационной безопасности, включая документы, регламентирующие деятельность работников подразделений Общества;
- получать информацию от работников подразделений Общества по вопросам применения информационных технологий и эксплуатации АС;
- участвовать в проработке технических решений по вопросам обеспечения информационной безопасности при проектировании и разработке программ;
- участвовать в испытаниях разработанных программ по вопросам оценки качества реали-

зации требований по обеспечению информационной безопасности.

- контролировать деятельность работников подразделений Общества по вопросам обеспечения информационной безопасности (включая контроль Internet трафика, внешней и внутренней почтовой переписки, содержимого файлов на дисках ПЭВМ и в личных каталогах на серверах).

Ответственным за информационную безопасность должны быть предоставлены права:

- доступ ко всем ресурсам АС с правами, достаточными для осуществления полного контроля АС.
- доступ во все помещения, где установлена аппаратура АС;
- запрет автоматизированной обработки информации при наличии непосредственной угрозы для защищаемой информации;
- запрет включения в число действующих новых элементов АС, если они не отвечают требованиям защиты информации и это может привести к серьезным последствиям в случае реализации значимых угроз информационной безопасности.

Ответственность за нарушения установленного порядка использования АС. Расследование нарушений.

Любое грубое нарушение порядка и правил работы в АС работниками структурных подразделений Общества и других организаций должно расследоваться. К виновным должны применяться адекватные меры воздействия. Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной автоматизированной обработки информации, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства Общества и его филиалов.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

- индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора, на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;
- проверка подлинности пользователей (аутентификация) на основе паролей, ключей на различной физической основе, биометрических характеристик личности и т.п.;
- регистрация (протоколирование) работы механизмов контроля доступа к ресурсам информационных систем с указанием даты и времени, идентификаторов запрашивающего и запрашиваемых ресурсов, вида взаимодействия и его результата;
- реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

8.2 Физические средства защиты

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

8.2.1 Разграничение доступа на территорию и в помещения

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение документов и информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

Более современными, надежными системами физической защиты, дающими широкие

возможности регистрации и контроля за доступом исполнителей и посторонних лиц в помещения, в которых проводятся работы и переговоры секретного (конфиденциального) характера, обрабатывается и хранится такая информация, являются технические системы, основанные на таких методах идентификации и аутентификации персонала как магнитные и электронные карты с личными данными, биометрические характеристики личности, реализуемые в виде автоматизированных систем контроля доступа в указанные помещения. Подобные автоматизированные системы могут быть реализованы в подразделениях безопасности, собирающих информацию с терминалов, контролирующих доступ в помещения, к объектам и отдельным средствам информатизации.

Для обеспечения физической безопасности компонентов АС необходимо осуществить ряд организационных и технических мероприятий, включающих (кроме выполнения рекомендаций по инженерной и технической защите зданий и помещений):

- введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки закрытой информации;
- оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

8.3 Технические (программно-аппаратные) средства защиты

Технические (программно-аппаратные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическую защиту информации и т.д.).

С учетом всех требований и принципов обеспечения информационной безопасности в АС по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства аутентификации пользователей и элементов АС (компьютеров, программ, баз данных и т.п.), соответствующих степени конфиденциальности информации и обрабатываемых данных;
- средства разграничения доступа к данным;
- средства криптографической защиты информации в линиях передачи данных и в базах данных;
- средства регистрации обращения и контроля использования защищаемой информации;
- средства ограничения использования внешних носителей информации;
- средства реагирования на обнаруженный НСД;
- средства маскировки от оптических средств наблюдения.

На технические средства защиты от НСД возлагается решение следующих основных задач (в соответствии с Руководящими документами ФСТЭК и ФСБ России, ГОСТ Р ИСО 27001 и ГОСТ Р ИСО 17799):

- идентификация и аутентификации пользователей при помощи имен и/или специальных аппаратных средств;
- регламентация доступа пользователей к физическим устройствам компьютера (дискам, портам ввода-вывода);
- избирательное управление доступом к логическим дискам, каталогам и файлам;
- полномочное (мандатное) разграничение доступа к защищаемым данным на рабочей станции и на файловом сервере;
- ограничение перечня разрешенных для запуска программ, расположенных как на локальных, так и на сетевых дисках;

- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;
- контроль целостности модулей системы защиты, системных областей диска и произвольных списков файлов в автоматическом режиме и по командам администратора;
- регистрация действий пользователя в защищенном журнале, наличие нескольких уровней детализации информации;
- централизованный сбор, хранение и обработка на файловом сервере журналов регистрации рабочих станций сети;
- защита данных системы защиты на файловом сервере от доступа всех пользователей, включая администратора сети;
- централизованное управление настройками средств разграничения доступа на рабочих станциях сети;
- оповещение администратора безопасности о событиях НСД, происходящих на рабочих станциях;
- оперативный контроль работы пользователей сети, изменение режимов функционирования рабочих станций и возможность блокирования (при необходимости) любой станции сети.

Успешное применение технических средств защиты предполагает, что выполнение перечисленных ниже требований обеспечено организационными мерами и используемыми физическими средствами защиты:

- физическая целостность всех компонентов АС обеспечена;
- каждый работник (пользователь АС) имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам АС;
- использование на компьютерах Общества инструментальных и технологических программ (тестовых утилит, отладчиков и т.п.), позволяющих предпринять попытки взлома или обхода средств защиты, ограничено и строго регламентировано;
- в защищенной системе нет программирующих пользователей. Разработка и отладка программ осуществляется за пределами защищенной системы;
- все изменения конфигурации технических и программных средств АС производятся в строго установленном порядке;
- сетевое оборудование (концентраторы, коммутаторы и т.п.) располагается в местах, недоступных для посторонних (специальные помещениях, шкафах, и т.п.).
- ИТ-подразделениями осуществляется непрерывное управление и административная поддержка функционирования средств защиты в соответствии с Планом защиты АС.

8.3.1 Средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей

В целях предотвращения работы с АС посторонних лиц необходимо обеспечить возможность распознавания системой каждого законного пользователя (или ограниченных групп пользователей). Для этого в системе (в защищенном месте) должен храниться ряд признаков каждого пользователя, по которым этого пользователя можно опознать. В дальнейшем при входе в систему, а при необходимости – и при выполнении определенных действий в системе, пользователь обязан себя идентифицировать, т.е. указать идентификатор, присвоенный ему в системе. Кроме того, для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, дискеты и т.п.

Аутентификация (подтверждение подлинности) пользователей должна осуществляться на основе использования паролей (секретных слов) или проверки уникальных характеристик (параметров) пользователей при помощи специальных биометрических средств.

8.3.2 Средства разграничения доступа зарегистрированных пользователей системы к ресурсам АС

После распознавания пользователя система должна осуществлять его авторизацию, то есть определять, какие права ему предоставлены: какие данные и как он может использовать, какие программы может выполнять, когда, как долго и с каких терминалов может работать, какие ресурсы системы может использовать и т.п. Авторизация пользователя должна осуществляется с использованием следующих механизмов реализации разграничения доступа:

- механизмов избирательного управления доступом, основанных на использовании атрибутных схем, списков разрешений и т.п.;
- механизмов полномочного управления доступом, основанных на использовании атрибутов конфиденциальности ресурсов и уровней допуска пользователей;
- механизмов обеспечения замкнутой среды доверенного программного обеспечения (индивидуальных для каждого пользователя списков разрешенных для запуска программ), поддерживаемых механизмами идентификации (распознавания) и аутентификации (подтверждения подлинности) пользователей при их входе в систему.

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны быть составной частью единой системы контроля доступа:

- на контролируемую территорию;
- в отдельные помещения;
- к элементам АС и элементам системы защиты информации (физический доступ);
- к ресурсам АС (программный доступ);
- к информационным хранилищам (носителям информации, внешним носителям информации, томам, файлам, наборам данных, архивам, справкам, записям и т.д.);
- к активным ресурсам (прикладным программам, задачам, формам запросов и т.п.);
- к операционной системе, системным программам и программам защиты и т.п.

8.3.3 Средства обеспечения и контроля целостности программных и информационных ресурсов

Контроль целостности программ, обрабатываемой информации и средств защиты, с целью обеспечения неизменности программной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной корректировки информации должен обеспечиваться:

- средствами подсчета контрольных сумм;
- средствами электронной цифровой подписи;
- средствами сравнения критичных ресурсов с их эталонными копиями (и восстановления в случае нарушения целостности);
- средствами разграничения доступа (запрет доступа с правами модификации или удаления).

В целях защиты информации и программ от несанкционированного уничтожения или искажения необходимо обеспечить:

- дублирование системных таблиц и данных;
- дуплексирование и зеркальное отображение данных на дисках;
- отслеживание транзакций (регистрация в соответствующих журналах);
- периодический контроль целостности операционной системы и пользовательских про-

грамм, а также файлов пользователей;

- антивирусную защиту;
- резервное копирование данных по заранее установленной схеме;
- хранение резервных копий вне выделенных помещений;
- обеспечение непрерывности электропитания для файл-серверов и критичных рабочих станций и кондиционирование электропитания для остальных рабочих станций.

8.3.4 Средства оперативного контроля и регистрации событий безопасности

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение политики безопасности и привести к возникновению кризисных ситуаций. Средства контроля и регистрации должны предоставлять возможности:

- ведения и анализа журналов регистрации событий безопасности (системных журналов). Журналы регистрации должны вестись для каждой рабочей станции сети;
- оперативного ознакомления администратора безопасности с содержимым системного журнала любой станции и с журналом оперативных сообщений об НСД;
- получения твердой копии (печати) системного журнала;
- упорядочения системных журналов по дням и месяцам, а также установления ограничений на срок их хранения;
- оперативного оповещения администратора безопасности о нарушениях.

При регистрации событий безопасности в системном журнале должна фиксироваться следующая информация:

- дата и время события;
- идентификатор субъекта (пользователя, программы), осуществляющего регистрируемое действие;
- действие (если регистрируется запрос на доступ, то отмечается объект и тип доступа).

Желательно, чтобы средства контроля обеспечивали обнаружение и регистрацию следующих событий:

- вход пользователя в систему;
- вход пользователя в сеть;
- неудачная попытка входа в систему или сеть (неправильный ввод пароля);
- подключение к файловому серверу;
- запуск программы;
- завершение программы;
- оставление программы резидентно в памяти;
- попытка открытия файла недоступного для чтения;
- попытка открытия на запись файла недоступного для записи;
- попытка удаления файла недоступного для модификации;
- попытка изменения атрибутов файла недоступного для модификации;
- попытка запуска программы, недоступной для запуска;
- попытка получения доступа к недоступному каталогу;
- попытка чтения/записи информации с диска, недоступного пользователю;
- попытка запуска программы с диска, недоступного пользователю;
- нарушение целостности программ и данных системы защиты
- и др.

Желательно поддерживать следующие основные способы реагирования на обнаруженные факты НСД (возможно с участием администратора безопасности):

- извещение владельца информации о НСД к его данным;
- снятие программы (задания) с дальнейшего выполнения;
- извещение администратора баз данных и администратора безопасности;
- отключение терминала (рабочей станции), с которого были осуществлены попытки НСД к информации;
- исключение нарушителя из списка зарегистрированных пользователей;
- подача сигнала тревоги и др.

8.3.5 Криптографические средства защиты информации

Одним из важнейших элементов системы обеспечения информационной безопасности АС должно быть использование криптографических методов и средств защиты информации от несанкционированного доступа при её передаче по каналам связи.

Все средства криптографической защиты информации в АС должны строиться на основе алгоритмов, соответствующих действующему ГОСТ 28147.

Ключевая система применяемых в АС шифровальных средств должна обеспечивать криптографическую живучесть и многоуровневую защиту от компрометации ключевой информации, разделение пользователей по уровням обеспечения защиты и зонам их взаимодействия между собой и пользователями других уровней.

Конфиденциальность и имитозащита информации при её передаче по каналам связи должна обеспечиваться за счет применения в системе шифросредств абонентского и на отдельных направлениях канального шифрования. Сочетание абонентского и канального шифрования информации должно обеспечивать её сквозную защиту по всему тракту прохождения, защищать информацию в случае её ошибочной переадресации за счет сбоев и неисправностей аппаратно-программных средств центров коммутации.

В АС, являющейся системой с распределенными информационными ресурсами, также должны использоваться средства формирования и проверки электронной цифровой подписи, обеспечивающие целостность и юридически доказательное подтверждение подлинности сообщений, а также аутентификацию пользователей, абонентских пунктов и подтверждение времени отправления сообщений. При этом должны использоваться только стандартизованные алгоритмы цифровой подписи (ГОСТ Р 34.10 и ГОСТ Р 34.11).

8.4 Защита информации от утечки по техническим каналам

В качестве основных мер защиты информации, циркулирующей в АС, рекомендуются:

- использование средств защиты информации;
- размещение объекта защиты относительно границы контролируемой зоны с учетом радиуса зоны возможного перехвата информации, полученного для данного объекта по результатам специальных исследований;
- конструктивные доработки технических средств и помещений, где они расположены, в целях локализации возможных каналов утечки информации;
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах контролируемой зоны;
- периодическая проверка технических средств на отсутствие паразитной генерации их элементов;
- создание выделенных сетей связи и передачи данных с учетом максимального затруднения доступа к ним посторонних лиц;
- развязка линий связи и других цепей между выходящими за пределы контролируемой зо-

ны и находящимися внутри нее;

- использование защищенных каналов связи.

Основными направлениями снижения уровня и информативности ПЭМИН являются:

- разработка и выбор оптимальных схем и элементов, основанных на применении устройств с низким уровнем излучения типа:
- жидкокристаллических и газоразрядных экранов отображения;
- оптико-электронных и волоконно-оптических линий передачи данных;
- экранирование (развязка) отдельных элементов и устройств АС, реализуемое путем:
- локального экранирования излучающих элементов СВТ и средств связи;
- экранирование кабелей и устройств заземления;
- применение развязывающих фильтров в цепях питания и т.п.;
- использование специальных программ и кодов, базирующихся:
- на применении мультипрограммных режимов обработки данных, обеспечивающих минимальные интервалы обращения к защищаемой информации.

8.5 Управление системой обеспечения информационной безопасности

Управление системой обеспечения информационной безопасности в АС представляет собой целенаправленное воздействие на компоненты системы обеспечения безопасности (организационные, технические, программные и криптографические) с целью достижения требуемых показателей и норм защищенности циркулирующей в АС информации в условиях реализации основных угроз безопасности.

Главной целью организации управления системой обеспечения информационной безопасности является повышение надежности защиты информации в процессе её обработки, хранения и передачи.

Целями управления системой обеспечения информационной безопасности являются:

- *на этапе создания, ввода в действие, модернизации и расширения АС:* разработка и реализация планов создания нормативно-правовых основ и технической базы, обеспечивающей использование передовых средств и информационных технологий обработки и передачи информации в интересах обеспечения информационной безопасности АС; организация и координация взаимодействия в этой области разработчиков АС, концентрация персонала, финансовых, материальных и иных ресурсов заинтересованных сторон при разработке и поэтапном вводе в действие системы; создание действенной организационной структуры, обеспечивающей комплексное решение задач информационной безопасности при функционировании АС оснащенной необходимыми программно-аппаратными средствами управления и контроля;
- *на этапе эксплуатации АС:* обязательное и неукоснительное выполнение предусмотренных на этапе создания АС правил и процедур, направленных на обеспечение информационной безопасности, всеми задействованными в системе участниками, эффективное пресечение посягательств на информационные ресурсы, технические средства и информационные технологии, своевременное выявление негативных тенденций и совершенствование управления в области защиты информации.

Управление системой обеспечения информационной безопасности реализуется специализированной подсистемой, представляющей собой совокупность органов управления, технических, программных и криптографических средств и организационных мероприятий и взаимодействующих друг с другом пунктов управления различных уровней.

Органами управления являются ИТ-подразделения, а пунктами управления – автоматизированные рабочие места администраторов (операторов), расположенные на объектах АС.

Функциями подсистемы управления являются: информационная, управляющая и вспомогательная.

Информационная функция заключается в непрерывном контроле состояния системы защиты, проверке соответствия показателей защищенности допустимым значениям и немедленном информировании ответственных о возникающих в АС ситуациях, способных привести к нарушению информационной безопасности. К контролю состояния системы защиты предъявляются два требования: полнота и достоверность. Полнота характеризует степень охвата всех средств защиты и параметров их функционирования. Достоверность контроля характеризует степень адекватности значений контролируемых параметров их истинному значению. В результате обработки данных контроля формируется информация состояния системы защиты, которая обобщается (агрегируется) и передается на вышестоящие пункты управления.

Управляющая функция заключается в формировании планов реализации технологических операций АС с учетом требований информационной безопасности в условиях, сложившихся для данного момента времени, а также в определении места возникновения ситуации уязвимости для информации и предотвращении её утечки за счет оперативного блокирования участков АС, на которых возникают угрозы информационной безопасности. К управляющим функциям администраторов безопасности относятся учет, хранение, и выдача документов и информационных носителей, паролей и ключей. При этом генерация паролей, ключей, сопровождение средств разграничения доступа, приемка включаемых в программную среду АС новых программных средств, контроль соответствия программной среды эталону, а также контроль над выполнением технологического процесса обработки конфиденциальной информации возлагается на администратора АС (базы данных).

К *вспомогательным функциям* подсистемы управления относятся учет всех операций, выполняемых в АС с защищаемой информацией, формирование отчетных документов и сбор статистических данных с целью анализа и выявления потенциальных каналов утечки информации.

8.6 Контроль эффективности системы защиты

Контроль эффективности защиты информации осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации.

Контроль может проводиться как выделенными работниками ИТ-подразделений (оперативный контроль в процессе информационного взаимодействия в АС), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

Контроль может осуществляться как с помощью штатных средств системы защиты информации от НСД, так и с помощью специальных программных средств контроля.

9. Первоочередные мероприятия по обеспечению информационной безопасности АС

Для реализации основных положений настоящей Политики целесообразно провести (осуществить) следующие мероприятия:

- для снижения затрат на создание системы защиты и упрощения категорирования подсистем АС рассмотреть возможность внесения изменений в конфигурацию сетей и СВТ, технологии обработки, передачи и хранения (архивирования) информации (с целью мак-

симального разделения компонентов АС, в которых обрабатывается информация различных категорий конфиденциальности);

- разработать конкретные требования к СЗИ АС и мероприятия по их реализации;
- определить возможность использования в АС имеющихся на рынке сертифицированных средств защиты информации;
- произвести закупку сертифицированных образцов и серийно выпускаемых технических и программных средств защиты информации и их внедрение на рабочих станциях и файловых серверах сети с целью контроля изменения конфигурации аппаратных и программных средств и действиями пользователей;
- произвести разработку программных средств защиты информации в случае, если на рынке отсутствуют требуемые программные средства;
- для обеспечения режима удаленного доступа пользователей по сети Общества к информации конфиденциальных баз данных рассмотреть возможность разработки специальных криптографических средств. На уровне прикладных программ необходимо разработать средства, обеспечивающие возможность доступа к конфиденциальным данным только с защищенных терминалов;
- определить степень участия персонала в обработке (передаче, хранении, обсуждении) информации, характер его взаимодействия между собой;
- произвести разработку организационно-распорядительной и рабочей документации по эксплуатации, а также средств и мер защиты информации в АС (План защиты, Инструкции, обязанности и т.п.), регламентирующих процессы допуска пользователей к работе с АС, разработки и использования программного обеспечения на рабочих станциях и серверах, порядок внесения изменений в конфигурацию аппаратных и программных средств при ремонте, развитии и обслуживании СВТ, порядок применения и администрирования средств защиты информации и т.п.;
- для снижения риска перехвата в сети с других рабочих станций имен и паролей привилегированных пользователей (в особенности администраторов средств защиты и баз данных) организовать их работу в отдельных сегментах сети, шире применять сетевые устройства типа switch (коммутатор), не использовать удаленных режимов конфигурирования сетевых устройств;
- исключить доступ программистов-разработчиков в эксплуатируемые подсистемы АС (к реальной информации и базам данных), организовать опытный участок АС для разработки и отладки программ. Передачу разработанных программ в эксплуатацию производить через библиотеку эталонного программного обеспечения ИТ-подразделения;
- для защиты компонентов ЛВС органов Общества от неправомерных воздействий из других ЛВС Общества и внешних сетей по IP-протоколу целесообразно использовать на узлах корпоративной сети Общества межсетевые экраны;
- произвести опытную эксплуатацию средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объектов информатизации и отработки технологических процессов обработки (передачи) информации;
- произвести специальную проверку выделенных помещений на предмет обнаружения, возможно, внедренных в эти помещения или предметы интерьера электронных устройств перехвата информации;
- произвести конструктивные доработки технических средств и помещений, где они расположены, в целях локализации возможных технических каналов утечки информации (в случае необходимости);
- произвести развязку линий связи и других цепей между выходящими за пределы контролируемой зоны и находящимися внутри нее;

- произвести классификацию защищенности АС от НСД к информации, предназначенных для обработки конфиденциальной информации;
- организовать физическую защиту объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности;
- организовать контроль состояния и эффективности защиты информации с оценкой выполнения требований нормативных документов организационно-технического характера, обоснованности принятых мер, проверки соблюдения норм защиты информации по действующим методикам с применением поверенной контрольно-измерительной аппаратуры и сертифицированных программных средств контроля.
- для контроля за состоянием защиты, выявлением уязвимостей в системе защиты серверов и рабочих станций и принятия своевременных мер по их устранению (исключению возможности их использования злоумышленниками) необходимо использовать специальные программы оценки защищенности (сканеры).

Список используемых сокращений

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система обработки информации
ВП	Выделенное помещение
ВТСС	Вспомогательные технические средства и системы
ГОСТ	Государственный стандарт
ЕСКД	Единая система конструкторской документации
ЕСПД	Единая система программной документации
ЗИ	Защита информации
ЛВС	Локальная вычислительная сеть
НГМД	Накопитель на гибком магнитном диске
НД	Нормативный документ
НЖМД	Накопитель на жестком магнитном диске
НСД	Несанкционированный доступ
ИБ	Информационная безопасность
ОС	Операционная система
ОТСС	Основные технические средства и системы
ПО	Программное обеспечение
ПС	Программные средства
ПЭВМ	Персональная ЭВМ
ПЭМИН	Побочные электромагнитные излучения и наводки
РД	Руководящий документ
РС	Рабочая станция
СВТ	Средства вычислительной техники
СЗИ НСД	Система защиты от НСД к информации
СЗСИ	Система защиты секретной информации
СКЗИ	Средство криптографической защиты информации
СПД	Сеть (система) передачи данных
СУБД	Система управления базами данных
ТЗ	Техническое задание
ТРП	Техноарбочий проект
ТС	Технические средства
БЭПО	Библиотека эталонного программного обеспечения
ЭВМ	Электронно-вычислительная машина
ЭМС	Электромагнитная совместимость

Термины и определения

Автоматизированная система обработки информации (АС) – организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, баз) данных на различных носителях, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей государственных органов, общественных или коммерческих организаций (юридических лиц), отдельных граждан (физических лиц) и иных потребителей информации.

Авторизованный субъект доступа – *субъект*, которому предоставлены соответствующие права доступа к объектам системы (полномочия).

Администратор безопасности – лицо или группа лиц, ответственных за обеспечение *безопасности* системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты.

Атака на автоматизированную систему – любое действие, выполняемое *нарушителем*, которое приводит к реализации *угрозы*, путем использования *уязвимостей АС*.

Безопасность – состояние защищенности жизненно важных интересов личности, предприятия, общества и государства от внутренних и внешних угроз. Безопасность достигается проведением единой политики в области охраны и защиты важных ресурсов, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства.

Информационная безопасность – защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Безопасность компьютерной информации – достижение требуемого уровня защиты (класса и категории защищенности) объекта информатизации при обработке информации и её передаче через сети передачи данных (СПД), обеспечивающего сохранение таких ее качественных характеристик (свойств), как: секретность (конфиденциальность), целостность и доступность.

Безопасность информационной технологии – защищенность технологического процесса переработки информации.

Безопасность субъектов информационных отношений – защищенность субъектов информационных отношений от нанесения им материального, морального или иного ущерба путем воздействия на информацию и/или средства ее обработки и передачи.

Безопасность АС (компьютерной системы) – защищенность АС от несанкционированного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, незаконной модификации или разрушения ее компонентов.

Безопасность информационного ресурса (в частности АС) – складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности.

Конфиденциальность заключается в том, что ресурс доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

Целостность, что ресурс может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) ресурса в любой момент времени.

Доступность информационного ресурса означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к нему.

Внешний воздействующий фактор – воздействующий фактор, внешний по отношению к объекту информатизации.

Внутренний воздействующий фактор – воздействующий фактор, внутренний по отношению к объекту информатизации.

Вредоносные программы – программы или измененные программы объекта информатизации (ОИ), приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ОИ.

Вспомогательные технические средства и системы (ВТСС) защищаемого объекта информатизации – технические средства и системы, не предназначенные для передачи, обработки и хранения секретной информации, устанавливаемые совместно с *ОТСС* или в выделенных помещениях.

К ним относятся:

- различного рода телефонные аппараты и системы;
- средства вычислительной техники;
- системы передачи данных в системе радиосвязи;
- системы охранной и пожарной сигнализации;
- системы оповещения и сигнализации;
- контрольно-измерительная аппаратура;
- системы кондиционирования;
- системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания; телевизоры и радиоприемники и т.д.);
- оргтехника;
- средства и системы электрочасофикации.

Выделенное помещение (ВП) – помещение для размещения технических средств защищенного объекта информатизации, а также помещение, предназначенное для проведения семинаров, совещаний, бесед и других мероприятий, в котором циркулирует конфиденциальная речевая информация.

Документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать, при этом, документирование информации является обязательным условием включения информации в информационные ресурсы.

Доступ к информации – ознакомление с информацией (копирование, тиражирование) или получение возможности ее обработки, её модификация (корректировка) или уничтожение (удаление). Доступ к информации регламентируется ее правовым режимом и должен сопровождаться строгим соблюдением его требований. Доступ к информации, осуществленный с нарушениями требований ее правового режима, рассматривается как несанкционированный доступ.

Доступность информации – свойство системы, в которой циркулирует информация (средств и технологии её обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежа-

щие полномочия.

Доступ к ресурсу – получение субъектом доступа возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данным ресурсом.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых необходимо для надежного обеспечения существования и возможности прогрессивного развития субъекта (личности, организации, общества или государства).

Замысел защиты – основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность мероприятий, необходимых для достижения цели защиты информации и объекта.

Защита информации (ЗИ) – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию (ГОСТ Р 50922).

Защита информации от несанкционированного доступа (НСД) – деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации (ГОСТ Р 50922).

Защищаемые объекты информатизации:

- средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы связи и передачи данных), технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео-, смысловой и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки секретной информации;
- технические средства и системы, не обрабатывающие непосредственно секретную информацию, но размещенные в помещениях, где обрабатывается (циркулирует) секретная информация;
- *выделенные помещения*, предназначенные для ведения секретных переговоров или в которых размещены средства закрытой телефонной связи.

Злоумышленник – *нарушитель*, действующий умышленно из корыстных побуждений.

Информация – сведения о лицах, предметах, фактах, событиях, процессах и явлениях независимо от формы их представления.

Информация в АС – сведения о лицах, фактах, событиях, процессах и явлениях в некоторой предметной области, включенные в систему обработки информации, или являющиеся ее результатом в различных формах представления на различных носителях и используемые (необходимые) для оптимизации принимаемых решений в процессе управления объектами данной предметной области.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта *секретная информация*, передаваемая, хранимая или обрабатываемая в *ОТСС* и обсуждаемая в *ВП*.

Компьютерная информация – информация в виде:

- записей в памяти ЭВМ, электронных устройствах, на машинных носителях (элементы, файлы, блоки, базы данных, микропрограммы, прикладные и системные программы, пакеты и библиотеки программ, микросхемы, программно-информационные комплексы и др.), обеспечивающих функционирование объекта информатизации (сети);

- сообщений, передаваемых по сетям передачи данных;
- программно-информационного продукта, являющегося результатом генерации новой или обработки исходной документированной информации, представляемого непосредственно на экранах мониторов ОИ, на внешних носителях данных (магнитные диски, магнитные ленты, оптические диски, дискеты, бумага для распечатки и т.п.) или через сети передачи данных;
- электронных записей о субъектах прав.

Контролируемая зона (КЗ) – это пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Границей КЗ могут являться:

- периметр охраняемой территории предприятия (учреждения);
- ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

В отдельных случаях на период обработки техническими средствами секретной информации (проведения закрытого мероприятия) КЗ временно может устанавливаться большей, чем охраняемая территория предприятия. При этом должны приниматься организационно-режимные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне;

Зона 2 - пространство вокруг *ОТСС*, на границе и за пределами которого напряженность электромагнитного поля информативного сигнала не превышает нормированного значения;

Зона 1 - пространство вокруг *ОТСС*, на границе и за пределами которого уровень наведенного от *ОТСС* информативного сигнала в *ВТСС*, а также в посторонних проводах и линиях передачи информации, имеющих выход за пределы контролируемой зоны, не превышает нормированного значения.

Конфиденциальная информация – информация, содержащая сведения, составляющие врачебную, коммерческую, служебную тайну или персональные данные, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Конфиденциальность информации – субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

Лицензия в области защиты информации – разрешение на право проведения тех или иных работ в области защиты информации (в соответствии с Постановление Правительства РФ от 15.08.2006 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»).

Нарушитель – это лицо (*субъект*), которое предприняло (пыталось предпринять) попытку *несанкционированного доступа* к ресурсам системы (попытку выполнения запрещенных ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства (чисто агентурные методы получения сведений, технические средства перехвата без модификации компонентов системы, штатные средства и недостатки систем защиты, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ и т.п.).

Несанкционированное действие – действие *субъекта* в нарушение установленных в системе правил обработки информации.

Несанкционированный доступ (НСД) – доступ *субъекта* к *объекту* в нарушение установленных в системе правил разграничения доступа.

Обработка информации в АС – совокупность операций (сбор, накопление, хранение, преобразование, отображение, выдача и т.п.), осуществляемых над информацией (сведениями, данными) с использованием средств АС.

Объект – пассивный компонент системы, единица ресурса автоматизированной системы (устройство, диск, каталог, файл и т.п.), доступ к которому регламентируется правилами разграничения доступа.

Основные технические средства и системы (ОТСС) защищаемого объекта информатизации – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи *секретной информации*. К ним могут относиться средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных), технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео-, смысловой и буквенно-цифровой информации), используемые для обработки секретной информации.

Пароль – служебное слово, которое считается известным узкому кругу лиц (одному лицу) и используется для ограничения доступа к информации, в помещение, на территорию.

Показатель эффективности защиты информации – мера или характеристика для оценки эффективности защиты информации (ГОСТ Р 50992).

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.

Разграничение доступа к ресурсам АС – это такой порядок использования ресурсов системы, при котором субъекты получают доступ к объектам в строгом соответствии с установленными правилами.

Руководящие документы ФСБ России – включают:

- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации;
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащих сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

Руководящие документы ФСТЭК России – включают:

- Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных;
- Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных;
- Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных;
- Рекомендации по обеспечению безопасности персональных данных при их обработке, в

информационных системах персональных данных.

- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)

Субъект – активный компонент системы (пользователь, процесс, программа), действия которого регламентируются правилами разграничения доступа.

Субъект информационных отношений – государство, государственные органы, государственные, общественные или коммерческие организации (объединения) и предприятия (юридические лица), отдельные граждане (физические лица) и иные субъекты, взаимодействующие с целью совместной обработки информации.

Угроза – реально или потенциально возможные действия по реализации опасных воздействующих факторов на АС с целью преднамеренного или случайного (неумышленного) нарушения режима функционирования объекта и нарушения свойств защищаемой информации или других ресурсов объекта.

Естественные угрозы – это угрозы, вызванные воздействиями на АС и ее элементы объективных физических процессов техногенного характера или стихийных природных явлений, не зависящих от человека;

Искусственные угрозы – это угрозы АС, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

- ***непреднамеренные (неумышленные, случайные) угрозы***, вызванные ошибками в проектировании АС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;
- ***преднамеренные (умышленные) угрозы***, связанные с корыстными устремлениями людей (*злоумышленников*).

Угроза автоматизированной системе – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба ресурсам АС.

Угроза информационной безопасности – случайное (неумышленное) или преднамеренное (злоумышленное) воздействие, приводящее к нарушению целостности, доступности и конфиденциальности информации или поддерживающей ее инфраструктуры, которое наносит ущерб собственнику, распорядителю или пользователю информации.

Угроза информационной безопасности – потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию.

Угроза интересам субъектов информационных отношений – потенциально возможное событие, действие, процесс или явление, которое посредством воздействия на информацию и другие компоненты АС может привести к нанесению ущерба интересам данных субъектов.

Уровень защиты (класс и категория защищенности) ОИ – характеристика, описываемая в нормативных документах определенной группой требований к данному классу и категории защищенности.

Уязвимость автоматизированной системы – любая характеристика АС, использование которой может привести к реализации угрозы.

Уязвимость информации – подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию.

Уязвимость субъекта информационных отношений – потенциальная подверженность субъекта нанесению ущерба его жизненно важным интересам посредством воздействия на критичную для него информацию, ее носители и процессы обработки.

Физический канал утечки информации – неконтролируемый физический путь от источника информации за пределы организации или круга лиц, обладающих охраняемыми сведениями, посредством которого возможно неправомерное (несанкционированное) овладение нарушителем защищаемой информацией.

Целостность информации – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Информационные способы нарушения информационной безопасности – включают:

- противозаконный сбор, распространение и использование информации;
- манипулирование информацией (дезинформация, сокрытие или искажение информации);
- незаконное копирование информации (данных и программ);
- незаконное уничтожение информации;
- хищение информации из баз данных;
- нарушение адресности и оперативности информационного обмена;
- нарушение технологии обработки данных и информационного обмена.

Программно-математические способы нарушения информационной безопасности – включают:

- внедрение программ-вирусов;
- внедрение программных закладок как на стадии проектирования системы (в том числе путем заимствования "зараженного" закладками программного продукта), так и на стадии ее эксплуатации, позволяющих осуществить несанкционированный доступ или действия по отношению к информации и системам ее защиты (блокирование, обход и модификация систем защиты, извлечение, подмена идентификаторов и т.д.) и приводящих к компрометации системы защиты информации.

Физические способы нарушения информационной безопасности – включают:

- уничтожение, хищение и разрушение средств обработки и защиты информации, средств связи, целенаправленное внесение в них неисправностей;
- уничтожение, хищение и разрушение машинных или других оригиналов носителей информации;
- хищение ключей (ключевых документов) средств криптографической защиты информации, программных или аппаратных ключей средств защиты информации от несанкционированного доступа;
- воздействие на обслуживающий персонал и пользователей системы с целью создания благоприятных условий для реализации угроз информационной безопасности;
- диверсионные действия по отношению к объектам информационной безопасности (взрывы, поджоги, технические аварии и т.д.).

Радиоэлектронные способы нарушения информационной безопасности – включают:

- перехват информации в технических каналах ее утечки (побочных электромагнитных излучений, создаваемых техническими средствами обработки и передачи информации, наводок в коммуникациях (сети электропитания, заземления, радиотрансляции, пожарной и охранной сигнализации и т.д.) и линиях связи, путем прослушивания конфиденциальных разговоров с помощью акустических, виброакустических и лазерных технических средств разведки, прослушивания конфиденциальных телефонных разговоров, визуального наблюдения за работой средств отображения информации);
- перехват и дешифрование информации в сетях передачи данных и линиях связи;
- внедрение электронных устройств перехвата информации в технические средства и помещения;

- навязывание ложной информации по сетям передачи данных и линиям связи;
- радиоэлектронное подавление линий связи и систем управления.

Организационно-правовые способы нарушения информационной безопасности – включают:

- закупку несовершенных, устаревших или неперспективных средств информатизации и информационных технологий;
- невыполнение требований законодательства и задержки в разработке и принятии необходимых нормативных правовых и технических документов в области информационной безопасности.

Система защиты АС (информации) – совокупность (комплекс) специальных мер правового (законодательного) и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения безопасности АС (циркулирующей в АС информации).

Цель защиты АС (информации) – предотвращение или минимизация наносимого ущерба (прямого или косвенного, материального, морального или иного) субъектам информационных отношений посредством нежелательного воздействия на компоненты АС, а также разглашения (утечки), искажения (модификации), утраты (снижения степени доступности) или незаконного тиражирования информации.

Правовые меры защиты информации – действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.

Морально-этические меры защиты информации – традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, репутации человека, группы лиц или организации. Морально-этические нормы бывают как неформальные (например, общепризнанные нормы честности и т.п.), так и оформленные в некоторый свод правил (устав) или предписаний.

Организационные (административные) меры защиты – это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.

Физические меры защиты – это разного рода механические, электро- или электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам АС и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.

Технические (аппаратно-программные) средства защиты – различные электронные устройства и специальные программы, входящие в состав АС, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).