ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА

Администрация Центрального района Санкт-Петербурга

Государственное бюджетное дошкольное образовательное учреждение
детский сад № 25 комбинированного вида Центрального района Санкт-Петербурга
(ГБДОУ детский сад № 25 Центрального района СПб)

«Принято»
Общим собранием работников
ГБДОУ детского сада № 25
Центрального района СПб
протокол от 27.08.2020 №1

«Утверждаю»
и.о.заведующего ГБДОУ детского сада № 25
Центрального района СПб
_____Шакурова Г.В.
приказ от 31.08.2020№ 103/1

ГБДОУ ДЕТСКИЙ САД № 25 ЦЕНТРАЛЬНОГО РАЙОНА СПБ

Подписано цифровой подписью: ГБДОУ ДЕТСКИЙ САД № 25 ЦЕНТРАЛЬНОГО РАЙОНА СПБ
Дата: 2022.06.30 17:20:03 +03'00'

Политика информационной безопасности ГБДОУ детский сад №25 Центрального района Санкт-Петербурга

Санкт-Петербург
2020

Содержание

Перечень сокращений

АРМ автоматизированное рабочее место

АС автоматизированная система

БД база данных

ВрП вредоносная программа

ВТСС вспомогательные технические средства и системы

ГИС геоинформационная система

ЗИ защищаемая информация

ИБ информационная безопасность

ИР информационный ресурс

ИТ информационная технология

КВ компьютерный вирус

КЗ контролируемая зона

КСЗИ комплексная система защиты информации

ЛВС локальная вычислительная сеть

МНИ машинные носители информации
МЭ межсетевой экран
НД нормативный документ
НСД несанкционированный доступ
ОИ объект информатизации
ОС операционная система
ОСПД объединенная сеть передачи данных
ОТСС основные технические средства и системы
ПИБ подсистема обеспечения информационной безопасности
ПК программный комплекс
ПО программное обеспечение
ПЭВМ персональная электронно-вычислительная машина
РД руководящий документ
РСД разрешительная система доступа
РПС разрушающее программное средство
РФ Российская Федерация
СУБД система управления базы данных
СВТ средства вычислительной техники
СЗИ система защиты информации
СКЗИ средства криптографической защиты информации
СУБД система управления базами данных
ФСБ федеральная служба безопасности
ФЗ федеральный закон
ЭлД электронный документ
ЭЦП электронная цифровая подпись

Основные понятия

информация - сведения (сообщения, данные) независимо от формы их представления;

информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

доступ к информации - возможность получения информации и ее использования;

конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах; (Пункт введен - Федеральный закон от 27.07.2010 № 227-ФЗ)
оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;
сайт в сети "Интернет" - совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет"; (Пункт введен - Федеральный закон от 28.07.2012 № 139-ФЗ; в редакции Федерального закона от 07.06.2013 № 112-ФЗ)
страница сайта в сети "Интернет" (далее также - интернет-страница) - часть сайта в сети "Интернет", доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети "Интернет"; (Пункт введен - Федеральный закон от 28.07.2012 № 139-ФЗ)
доменное имя - обозначение символами, предназначенное для адресации сайтов в сети "Интернет" в целях обеспечения доступа к информации, размещенной в сети "Интернет"; (Пункт введен - Федеральный закон от 28.07.2012 № 139-ФЗ)
сетевой адрес - идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему; (Пункт введен - Федеральный закон от 28.07.2012 № 139-ФЗ)
владелец сайта в сети "Интернет" - лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети "Интернет", в том числе порядок размещения информации на таком сайте; (Пункт введен - Федеральный закон от 28.07.2012 № 139-ФЗ)
провайдер хостинга - лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети "Интернет"; (Пункт введен - Федеральный закон от 28.07.2012 № 139-ФЗ)
единая система идентификации и аутентификации - федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах; (Пункт введен - Федеральный закон от 07.06.2013 № 112-ФЗ)
поисковая система - информационная система, осуществляющая по запросу пользователя поиск в сети "Интернет" информации определенного содержания и предоставляющая пользователю сведения об указателе страницы сайта в сети "Интернет" для доступа к запрашиваемой информации, расположенной на сайтах в сети "Интернет", принадлежащих иным лицам, за исключением информационных систем, используемых для осуществления государственных и муниципальных функций, оказания

государственных и муниципальных услуг, а также для осуществления иных публичных полномочий, установленных федеральными законами. (Пункт введен - Федеральный закон от 13.07.2015 № 264-ФЗ)

Назначение и правовая основа политики информационной безопасности

Настоящая политика информационной безопасности (ИБ) разработана на основе требований действующих в Российской Федерации законодательных и нормативных документов, приведенных в разделе «Нормативные документы», регламентирующих вопросы защиты информации Организации, с учетом современного состояния, целей, задач и правовых основ создания, эксплуатации и функционирования информационной системы.

Положения и требования Политики распространяются на все структурные подразделения ГБДОУ детский сад № 25 Центрального района СПб, основных разработчиков и исполнителей, которые участвуют в разработке, создании, развертывании, вводе в эксплуатацию информационной системы, в части их касающейся.

Положения и требования Политики могут быть распространены (по согласованию) также на другие предприятия, учреждения и организации, осуществляющих информационное взаимодействие в качестве поставщиков и потребителей (пользователей) информации.

Под **информационной безопасностью** информационной системы понимается состояние защищенности информационной среды (информации, информационных ресурсов, фондов и информационных систем, баз данных), при которой её формирование, использование, развитие и информационный обмен обеспечивается защитой информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования.

Политика ИБ является методологической основой для:

- разработки подсистемы информационной безопасности (далее именуется — ПИБ) при доступе к информации, реализуемой на объектах информатизации с ограниченным доступом, в виде комплексной системы защиты информации от несанкционированного доступа — КСЗИ НСД;
- разработки защищенного электронного документооборота, с использованием средств криптографической защиты информации, развертывания системы удостоверяющих центров, применения электронной цифровой подписи и частных виртуальных сетей обмена защищаемой информации;
- разработки конкретных нормативных документов и мероприятий, регламентирующих деятельность в области обеспечения информационной безопасности;
- реализации прав граждан, организаций и государства на получение, распространение и использование информации.

Политика обеспечения информационной безопасности основывается на следующих основных принципах:

- соблюдение Конституции Российской Федерации, законов Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности;
- достижение целей, описанных в уставном положении Организации;
- открытость процессов, и информирование лиц, принимающих решения;
- приоритетное развитие отечественных и свободных современных информационных и телекоммуникационных технологий, в том числе в защищенном исполнении;
- правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

- определение и поддержание требуемого баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;
- оценка состояния информационной безопасности, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, парирования и нейтрализации этих угроз;
- применение сертифицированных средств защиты информации и лицензирование деятельности в области защиты информации;
- совершенствование и развитие системы подготовки кадров в области информационной безопасности.

Основные сведения об информационной системе

Информационные системы Организации предназначены для обеспечения эффективного достижения целей Организации посредством эффективного использования ресурсов, современного управления и технологий.

Информационные системы Организации включают в себя средства информатизации — программно-технические комплексы и телекоммуникационные средства, обеспечивающие доступ к данным, а также организационно-правовое, методическое и технологическое обеспечение её создания и функционирования.

Информационная система развивается как автоматизированные рабочие места, взаимосвязь между которыми осуществляется через съемные носители данных.

Ряд объектов информатизации осуществляет взаимодействие с внешними (государственными и общественными) организациями по коммутируемым каналам с использованием средств передачи информации.

Программно-технические комплексы на автоматизированных рабочих местах включает технические средства обработки данных (ПЭВМ), средства обмена данными с возможностью выхода в сеть интернет (модемы), а также средства хранения информации (резервирования, дублирования и архивирования).

В технологическом плане объекты информатизации включают:

- технологическое оборудование (сетевое оборудование - модемы);
- программные средства (операционные системы, системы управления базами данных, общесистемное и прикладное программное обеспечение);
- информационные ресурсы, содержащие открытые сведения, сведения конфиденциального характера, представленные в виде документов в электронной форме (электронный документ), на бумажной и иной основе или записей на носителях на магнитной, оптической и другой физической основе, информационных массивов и баз данных;
- средства связи и передачи данных (интернет);
- каналы связи (телефон и факс);
- служебные режимные и выделенные помещения (где это необходимо), в которых обрабатывается документированная информация с ограниченным доступом;
- технические средства и системы, не обрабатывающие информацию (вспомогательные технические средства и системы — ВТСС), размещенные в помещениях, где обрабатывается (циркулирует) документированная информация, содержащая сведения с ограниченным доступом;
- средства защиты информации от несанкционированного доступа.

В процессе функционирования информационная система должна обеспечить:

- сбор и обработку информации на всех уровнях;
- ведение баз данных информации и информационное обслуживание Организации и ее деловых партнёров;
- организацию обмена сведениями на уровне межкорпоративного взаимодействия, а также обслуживания организаций и отдельных граждан;
- информационную безопасность на объектах информатизации, где ведется обработка документированной информации с ограниченным доступом, в виде КСЗИ НСД.

Основными объектами защиты в информационной системе являются:

- информационные ресурсы с ограниченным доступом, содержащие сведения конфиденциального характера (служебная информация, персональные данные) и иные информационные ресурсы (в том числе открытая информация), представленные в виде документов, баз данных;
- система формирования, распространения и использования информации, информационные технологии, процедуры сбора, обработки, хранения и передачи информации, пользователи системы и её обслуживающий персонал;
- информационная инфраструктура, включающая центры обработки и анализа информации (данных), технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена, КСЗИ НСД, документация на них и другая, относящаяся к ним информация, здания и помещения, в которых проводится обработка документированной информации с ограниченным доступом или переговоры конфиденциального характера;
- технологические процессы обработки, передачи и хранения информации по ведению документов, управленческой, отчётной и статистической информации.

Категории информационных ресурсов и роли пользователей

В данном разделе описаны основные информационные артефакты политики информационной безопасности.

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Информация, размещаемая ее обладателями в сети "Интернет" в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в форме открытых данных. (часть 4 введена Федеральным законом от 07.06.2013 N 112-ФЗ)

Информация в форме открытых данных размещается в сети "Интернет" с учетом требований законодательства Российской Федерации о государственной тайне. В случае, если размещение информации в форме открытых данных может привести к распространению сведений, составляющих государственную тайну, размещение указанной информации в форме открытых данных должно быть прекращено по требованию органа, наделенного полномочиями по распоряжению такими сведениями. (часть 5 введена Федеральным законом от 07.06.2013 N 112-ФЗ)

В случае, если размещение информации в форме открытых данных может повлечь за собой нарушение прав обладателей информации, доступ к которой ограничен в соответствии с федеральными законами, или нарушение прав субъектов персональных данных, размещение указанной информации в форме открытых данных должно быть прекращено по решению суда. В случае, если размещение информации в форме открытых данных осуществляется с нарушением требований Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных", размещение информации в форме открытых данных должно быть приостановлено или прекращено по требованию уполномоченного органа по защите прав субъектов персональных данных. (часть 6 введена Федеральным законом от 07.06.2013 N 112-ФЗ)

Категории информационных ресурсов, подлежащих защите

Перечень и необходимый уровень защиты обрабатываемых информационных ресурсов содержащих сведения, составляющие конфиденциальную информацию (служебную информацию, персональные данные), определяется следующим образом:

- перечень сведений, отнесенных к служебной информации, определяется пометкой «Для служебного пользования»;
- перечень сведений, отнесенных к персональным данным, определяется в соответствии с 152-ФЗ «О персональных данных»;
- необходимый уровень защиты определяется, в соответствии с требованиями основных документов.

Открытые информационные ресурсы — информация, которая не отнесена к категории ограниченного доступа. Открытые информационные ресурсы с точки зрения ограничения доступа разделяются на следующие категории:

- *регламентируемые* ресурсы — информационные ресурсы, доступ к которым требует выполнения определенных процедур (например, получение разрешения — визирования), или доступ к которым свободен, а право копирования ограничено на основании авторского права;
- *свободные* ресурсы — информационные ресурсы, доступ к которым свободен для всех пользователей (в том числе и внешних) и которые разрешено свободно копировать, модифицировать и распространять.

Категории информации, подлежащие защите		
Категория (тип) сведений (информации)	**Документы, определяющие состав и объем сведений (информации)**	**Требования по защите**
Персональные данные	Состав и объем определяется Федеральным законом «О персональных данных» и «Перечнями сведений, отнесенных к персональным данным (информация о гражданах)». *Примечание:* Персональные данные — сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность	Защита обязательна
Открытые регламентные ресурсы	Состав и объем определяется руководством учреждения	Уровень защиты определяется руководством.

Разрешительная ролевая система доступа к информации

Пользователями информационных ресурсов (в части их касающейся) являются:

- органы государственной власти и местного самоуправления;
- налоговые органы в пределах территории, находящейся под их юрисдикцией;
- суды и правоохранительные органы, имеющие в производстве дела, связанные с деятельностью Организации;
- партнёры организации;
- работники Организации;
- иные лица, устанавливаемые законодательством Российской Федерации.

На *объектах информатизации имеются следующие основные категории пользователей* (в части их касающейся), которые должны иметь различные полномочия по доступу к информационным, программным и другим ресурсам:

- лица, заинтересованные в получении сведений;
- пользователи прикладного программного обеспечения и СУБД баз данных (конечные пользователи предприятий, организаций и учреждений);

- ответственные лица за ведение баз данных (ввод, корректировка, удаление, архивирование, резервирование, дублирование данных БД);
- разработчики прикладного программного обеспечения;
- специалисты по обслуживанию технических средств вычислительной техники;
- администраторы и специалисты по защите информации (информационной безопасности);
- должностные лица, осуществляющие технологические процедуры.

На всех объектах информатизации в соответствии с действующими нормативными документами должна быть разработана разрешительная система доступа.

Угрозы информационной безопасности

В данном разделе рассматриваются и классифицируются угрозы информационной безопасности.

Источники и угрозы информационной безопасности на объектах информатизации

Основными источниками защищаемой информации на объектах информатизации (ОИ) являются субъекты информационных отношений:

- пользователи (операторы), администраторы АС (ЛВС), руководители разработки и эксплуатации АС, технический (обслуживающий) персонал;
- документы на твердой основе, различного характера и назначения включая электронные документы на машиночитаемых носителях информации, с защищаемой информацией;
- штатные технические средства АС обработки защищаемой информации: АРМ, средства обеспечения производственной деятельности людей, информационные и телекоммуникационные линии связи.

Под угрозами информационной безопасности понимается потенциальная возможность нарушения её следующих основных, качественных характеристик (свойств):

- конфиденциальности (разглашение, утечка) сведений, составляющих служебную тайну, а также персональных данных;
- работоспособности (дезорганизация работы) программно-технических комплексов, блокирование информации, нарушение технологических процессов обработки информации, срыв своевременного решения выполняемых задач;
- целостности и достоверности информационных, программных и других ресурсов, а также фальсификация (подделка) документов.

Источники угроз информационной безопасности, разделяются на *внешние и внутренние*:

К внешним источникам угроз относятся:

- деятельность иностранных разведывательных и специальных служб, направленная на добывание защищаемых информационных ресурсов с ограниченным доступом, на подрыв авторитета Организации;
- действия преступных групп, формирований и связанных с ними коррумпированных лиц по добыванию защищаемой информации в целях реализации своих преступных замыслов;
- использование средств опасного воздействия на информационные ресурсы, получение несанкционированного доступа к ним;
- преступная деятельность отдельных лиц, бандитских групп и формирований или злоумышленников, конкурирующих и недобросовестных организаций, в том числе с использованием телекоммуникационных систем (прежде всего Интернет);
- диверсионные действия по отношению к объектам информатизации (поджоги, технические аварии, взрывы и т.д.);
- деятельность министерств и ведомств и субъектов Российской Федерации, препятствующая или умышленно создающая трудности работе системы, совершаемая в противовес принятых законодательных актов;
- стихийные бедствия, аварии, и техногенные катастрофы.

К внутренним источникам угроз относятся:

- неправомерные действия должностных лиц в области формирования, распространения и использования защищаемой информации;

- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия персонала, работающего на объектах информатизации;
- отказы технических средств и программного обеспечения в информационных и телекоммуникационных системах;
- некомпетентные действия и ошибки, допущенные при эксплуатации информационных систем;
- халатность и недостаточно четкое исполнение служебных обязанностей при проведении мероприятий по защите информации;
- нарушения пользователями (исполнителями работ) и обслуживающим персоналом установленных регламентов сбора, обработки и передачи информации, а также требований по защите информации;
- отказы, неисправности и сбои средств защиты информации и средств контроля эффективности, принятых мер по защите информации;
- непреднамеренные (ошибочные, случайные, необдуманные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия персонала при эксплуатации объектов информатизации, приводящие к разглашению защищаемой информации;
- некоординированность или отсутствие необходимых сил и финансовых средств, для реализации мер в организации и защите информационных ресурсов;
- противозаконная деятельность коммерческих и экономических структур, имеющих позиции в среде сотрудников и пользователей;
- получение криминальными структурами доступа к защищаемой информации, снижение степени защищенности законных интересов граждан, общества и государства в информационной сфере.

Классификация, способы реализации и природа возникновения угроз информационной безопасности на объектах информатизации

Потенциальные угрозы безопасности защищаемой информации на объектах информатизации **по сфере воздействия**, с точки зрения их нахождения вне или внутри ОИ, при его создании и функционировании разделяются на *внешние* и *внутренние*.

Внешние угрозы исходят от субъектов (источников) — внешних, возможных нарушителей, приведенных в разделе 5.

Внутренние угрозы исходят от субъектов (источников) — внутренних, возможных нарушителей, приведенных в разделе 5.

Потенциальные угрозы, по *отношению к компонентам* объекта информатизации (АРМ) с защищаемой информацией, могут реализовываться следующими основными **способами**:

- информационными;
- программно-математическими;
- физическими;
- организационно-правовыми.

Информационные способы реализации угроз включают:

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

Программно-математические способы реализации угроз включают:

- удаленное проникновение;
- локальное проникновение;
- удаленный отказ в обслуживании;

- локальный отказ в обслуживании;
- взлом паролей
- внедрение компьютерных вирусов;
- внедрение программных закладок как на стадии разработки программного обеспечения (в том числе путем заимствования «зараженного» закладками программного продукта), так и на стадии эксплуатации ПО, позволяющих осуществить НСД по отношению к информации и системе её защиты (включая блокирование, обход и модификацию средств защиты информации от НСД, извлечение, подмена идентификаторов) и приводящих к компрометации СЗИ от НСД.

Физические способы реализации угроз включают:

1. уничтожение, хищение и разрушение средств обработки и защиты защищаемой информации, информационных линий связи ОИ, целенаправленное внесение в них неисправностей;
2. уничтожение, хищение и разрушение машинных или других оригиналов носителей защищаемой информации;
3. хищение программных или аппаратных ключей (реквизитов) средств защиты информации от НСД;
4. воздействие на персонал ОИ с целью создания благоприятных условий для реализации угроз;
5. диверсионные действия по отношению к компонентам ОИ, включая взрывы, поджоги, технические аварии.

Организационно-правовые способы реализации угроз включают:

1. использование несовершенных, устаревших или неперспективных СВТ и информационных технологий;
2. невыполнение требований законодательства Российской Федерации и задержка в разработке и принятии необходимых нормативных, правовых, организационно-распорядительных и эксплуатационных документов в области информационной безопасности.

Результатом реализации угроз на ОИ являются:

- нарушение *конфиденциальности* защищаемых сведений (разглашение, утрата, хищение, утечка, перехват и т.п.);
- нарушение *целостности* защищаемой информации (уничтожение, искажение, подделка и т.п.);
- нарушение регламентируемой *доступности* к защищаемой информации и работоспособности программно-технических комплексов ОИ.

Потенциальные угрозы на объектах информатизации, **по природе их возникновения**, разделяются на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы — угрозы, вызванные воздействиями на ОИ и её компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы — угрозы на ОИ, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

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

Основные искусственные, непреднамеренные угрозы на ОИ — действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без корыстного или злого интереса.

Основные искусственные, преднамеренные угрозы на ОИ — действия, совершаемые людьми умышленно для дезорганизации работы, вывода ОИ или его компонент из строя, проникновения в ОИ для реализации несанкционированного доступа к защищаемой

информации. Для достижения поставленной цели возможный нарушитель может использовать не одну, а некоторую совокупность угроз.

Искусственные угрозы

Непреднамеренные угрозы на ОИ	**Преднамеренные угрозы на ОИ**
Неумышленные действия, приводящие к частичному или полному отказу или разрушению технических, программных, информационных ресурсов ОИ. Неумышленная порча оборудования, удаление, искажение файлов с защищаемой информацией или программ, в том числе системных. Неправомерное отключение оборудования или изменение режимов работы устройств и программ. Неумышленная порча носителей информации. Запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности ОИ или его компонент (зависания или зацикливания) или осуществляющих необратимые изменения (форматирование или реструктуризацию МНИ, удаление данных и т.п.). Нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях). Заражение ПЭВМ компьютерными вирусами. Неосторожные действия, приводящие к разглашению защищаемой информации или делающие её общедоступной. Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей, идентификационных карточек, пропусков и т.п.). Проектирование архитектуры ОИ, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности ОИ и СЗИ от НСД. Игнорирование организационных ограничений (установленных правил) при работе на ОИ.	Физическое разрушение ОИ (путем взрыва, поджога и т.п.) или вывод из строя отдельных наиболее важных компонент (устройств, носителей важной системной информации, и т.п.). Отключение или вывод из строя подсистем обеспечения функционирования ОИ (электропитания, охлаждения и вентиляции, линий связи). Действия по дезорганизации функционирования ОИ (изменение режимов работы устройств или программ). Вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей ОИ, имеющих определенные полномочия. Применение устройств дистанционной фото- и видео съемки. Перехват данных, передаваемых по информационным линиям связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения на ОИ. Хищение технических средств и носителей информации (системных блоков ПЭВМ, МНИ, запоминающих устройств). Несанкционированное копирование носителей информации, включая МНИ. Хищение производственных отходов (распечаток, записей, списанных МНИ). Чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств ПЭВМ. Чтение информации из областей оперативной памяти, используемых операционной системой (в том числе СЗИ от НСД) или другими пользователями, в асинхронном режиме используя недостатки многозадачных операционных систем и систем программирования. Незаконное получение паролей и других реквизитов разграничения доступа (используя халатность пользователей, путем подбора, путем имитации интерфейса обмена) с последующей маскировкой под зарегистрированного пользователя («маскарад»).

Некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности. Пересылка данных по ошибочному адресу абонента (устройства). Ввод ошибочных данных. Неумышленное повреждение информационных линий связи.	Несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи. Внедрение вредоносного программного кода («закладок», «вирусов», «троянских коней», «кейлогеров», «жучков»), то есть такого исполняемого 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 ОИ. Незаконное подключение к информационным линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений. Незаконное подключение к информационным линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в ЛВС и успешной аутентификации с последующим вводом и навязыванием ложных сообщений. Воздействие на технические и программные средства в целях нарушения адресности и своевременности информационного обмена в ЛВС.

Технические каналы утечки защищаемой информации

Технические каналы утечки информации разделяют на косвенные и прямые.

Под *косвенными* понимаются технические каналы утечки информации, использование которых не требует проникновения в помещения, где расположены компоненты ОИ. Для использования прямых каналов такое проникновение необходимо.

Прямые технические каналы утечки информации могут использоваться без внесения изменений в компоненты ОИ или с изменениями компонентов.

По типу основного средства, используемого для реализации угрозы (атакующего воздействия), все технические каналы можно условно разделить на три группы:

- с помощью человека;
- с помощью программы;
- с помощью технических средств (аппаратуры).

Технические каналы утечки информации ОИ в общем, виде могут быть сведены в следующие группы:

- визуально-оптические (визуальный обзор документов, просмотр информации с экранов дисплеев и других средств её отображения с помощью фото и видеосъемки);
- акустические;
- электромагнитные (магнитные, электрические);
- материально-вещественные.

От каждого источника защищаемая информация по техническим каналам утечки может попасть к нарушителю.

Нарушители, совершая действия с преднамеренными или непреднамеренными угрозами и используя соответствующие способы реализации угроз, осуществляют несанкционированный доступ по техническим каналам утечки к защищаемой информации.

Для защиты информации от угроз информационной безопасности, осуществления несанкционированного доступа по техническим каналам утечки, на каждом объекте информатизации разрабатывается и применяется комплексная система защиты информации от несанкционированного доступа — КСЗИ НСД, объединяемая в подсистему информационной безопасности.

Модель возможного нарушителя на объектах информатизации

В данном разделе построена модель возможного нарушителя информационной безопасности.

Категории возможных нарушителей

Разработка модели возможного нарушителя на объектах информатизации проведена в соответствии с основными положениями документа: «Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» (Гостехкомиссия России, 1992г.).

В соответствии с указанным документом принимаются следующие основные положения:

- В качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами ОИ.
- Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами ОИ. Выделяется четыре уровня этих возможностей.

Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в ОИ — запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием ОИ, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств ОИ, вплоть до включения в состав программно-технических комплексов собственных технических средств с новыми функциями по обработке информации.

В своем уровне нарушитель является специалистом высшей квалификации, знает все о ОИ и, в частности, о системе и средствах её защиты.

Под **возможным нарушителем** (злоумышленником) для объектов информатизации подразумевается лицо или группа лиц, не состоящих или состоящих в сговоре, которые в результате преднамеренных или непреднамеренных действий потенциально могут нанести ущерб защищаемым ресурсам (информации).

Для принятия мер по обеспечению информационной безопасности защищаемой информации на объектах информатизации (обрабатывающих информацию с ограниченным доступом) в разрабатывается **модель возможного нарушителя** (применительно к конкретному ОИ), которая включает две категории возможных нарушителей — *внешние и внутренние возможные нарушители*.

Категории возможных нарушителей на ОИ

Уровень	**Внешние, возможные нарушители**	**Внутренние, возможные нарушители**
I	Посетители	Пользователи (операторы)

II	Уволенные работники организации	
III	Хакеры	Администраторы и специалисты по защите информации
IV	Криминальные группировки и сторонние организации	Руководители разработки и эксплуатации ОИ, технический (обслуживающий) персонал

Предполагается, что несанкционированный доступ на объекты информатизации посторонних лиц исключается организационными мерами (охрана территории).

К внешним возможным нарушителям относится деятельность по добыванию конфиденциальной информации. При этом внешний возможный нарушитель ведет перехват, анализ и модификацию информации, передаваемой по каналам связи ОИ, проходящим вне контролируемой территории.

Предположения о квалификации внешнего возможного нарушителя:

- является высококвалифицированным специалистом в области съема и обработки информации с проводных линий связи и радиоканалов;
- знает сетевое и канальное оборудование, протоколы передачи данных, используемые в программно-технических комплексах;
- знает особенности системного и прикладного программного обеспечения, а также технических средств;
- знает функциональные особенности работы ОИ, формирования массивов информации и потоков запросов к ним;
- знает специфику задач, и структуру ОИ.

Возможность создания коалиций нарушителей (внутренних и внешних, внешних и внутренних), должна исключаться с помощью проведения службой безопасности и кадровой службы организационных мероприятий.

Особенности возможных нарушителей

Каждый уровень возможных нарушителей характеризуется следующими параметрами:

- квалификация возможного нарушителя;
- техническая оснащённость, финансовые возможности возможного нарушителя;
- категории лиц, к которым может принадлежать возможный нарушитель;
- данные, необходимые возможному нарушителю и период их актуальности;
- количественная оценка времени, которое возможный нарушитель может затратить для преодоления системы (средств) защиты.

Внешние возможные нарушители

Невозможность пребывания внешних возможных нарушителей в помещениях с программно-техническими комплексами ОИ *без контроля* со стороны работников Организации обеспечивается организационно.

Посетители

Посетители, находясь на территории (в помещениях) ОИ организации могут случайно, или целенаправленно:

- стать свидетелем конфиденциальных переговоров между сотрудниками организации;
- получить доступ к защищаемой информации на бумажных носителях (например, путем визуального обзора разложенных документов на столах работников организации, фотографирования);
- получить случайный доступ к АРМ ;
- проникнуть в защищаемые помещения организации, во вне рабочее время.

Уволенные работники организации

Уволенные работники организации могут обладать специфическими возможностями, основанными на осведомленности о структуре организации и ОИ в целом, неизмененных правах по доступу к защищаемой информации. Возможна продажа третьим лицам украденной документации и МНИ с защищаемой информацией.

Хакеры

Хакеры (не смотря на малочисленность) несут большую потенциальную опасность, в связи с высокой профессиональной квалификацией. В случае найма хакеров криминальными группировками или сторонними организациями (осуществляющих экономический или промышленный шпионаж), а также взаимодействия с внутренними нарушителями в организации они являются опасными нарушителями. Хакеры получив информацию о проходящих информационных потоках, могут создать ситуации по скрытому получению защищаемой информации (в течении длительного периода времени), проводить модификацию или уничтожение данных и программного обеспечения, препятствовать штатному функционированию СВТ.

Криминальные группировки и сторонние организации

Криминальные группировки и сторонние организации (осуществляющие экономический или промышленный шпионаж) являются самими опасными, так как обладают значительными финансовыми и техническими возможностями и будут стараться получить защищаемую информацию всеми возможными способами: путем взлома защищенных программ на АРМ, подкупа или шантажа работников организации. Нарушителей данной группы достаточно сложно обнаружить, поскольку ущерб от утечки защищаемой информации может быть неявный, цели нарушителей могут быть рассчитаны на долгосрочную перспективу.

Распространенными действиями являются подкуп должностных лиц, позволяющий получать защищаемую информацию (например, в виде копий резервных магнитных носителей информации) по текущему состоянию всех баз данных. В случае подкупа руководящих работников — получение информации о текущих целях, планах, решениях, стратегии организации. Возможен наем хакеров для проведения спланированных атак с целью получения защищаемой информации из организации.

Внутренние возможные нарушители

Невозможность нанесения существенного вреда внутренними возможными нарушителями обеспечивается организационно.

Пользователи (операторы)

Пользователи (операторы), несмотря на свою многочисленность и постоянную возможность доступа к базам данных, не являются опасными. При правильной организации работы в АРМ, все действия пользователей (операторов) протоколируются, доступ к персональным компьютерам (АРМам) и базам данных ограничен и не превышает уровень необходимый для выполнения производственных задач.

Администраторы ЛВС и специалисты по защите информации

Администраторы по защите информации являются опасной группой среди внутренних нарушителей, в связи с высокой профессиональной квалификацией и спецификой выполняемых задач, не смотря на свою малочисленность. В частности, ими могут быть созданы ситуации, препятствующие штатному функционированию СВТ (остановки, сбой; уничтожение и/или модификация программного обеспечения для внесения программных закладок; создания множественных, ложных информационных сообщений).

Руководители разработки и эксплуатации ОИ

Руководители разработки и эксплуатации ОИ, являются потенциально опасными в первую очередь из-за наличия больших прав по доступу в ЛВС и в силу больших руководящих полномочий. Кроме того, учет и протоколирование действий руководителей, смена личных паролей (идентификаторов) по доступу в ЛВС часто не выполняются должным образом. Это может привести к несанкционированному доступу к защищаемой информации посторонних пользователей, через подбор пароля и выполнение действий от лица руководителя.

Цели и задачи обеспечения информационной безопасности

Основными целями обеспечения информационной безопасности, являются:

1. защита субъектов информационных отношений (интересы которых затрагиваются при создании и функционировании информационной системы) от возможного нанесения им ощутимого материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования объектов информатизации или несанкционированного доступа к циркулирующей в ней информации и её незаконного использования;
2. обеспечение соблюдения требований законодательства, руководящих и нормативных документов и общей политики безопасности;
3. обеспечение работоспособности подсистемы информационной безопасности;
4. обеспечение требований и условий целостности и конфиденциальности информации циркулирующей в системе.

   Указанная цель достигается посредством обеспечения (поддержания) следующих свойств информации при её автоматизированной обработки:

- доступности обрабатываемой информации для зарегистрированных пользователей, устойчивого функционирования системы, 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 и передаваемой по каналам связи;
- целостности и аутентичности (подтверждение авторства) информации, хранимой, обрабатываемой и передаваемой по каналам связи.

  Основными задачами, реализуемыми *подсистемой информационной безопасности (с входящими в её состав КСЗИ НСД каждого объекта информатизации)* являются:

- своевременное выявление и прогнозирование внутренних и внешних угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений;
- выявление попыток несанкционированного доступа к информационным ресурсам;
- выполнение централизованного комплекса мер по противодействию техническим разведкам и предотвращения НСД к защищаемой информации и БД;
- предупреждение преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе её создания, обработки, передачи и хранения;
- разработка и эксплуатация информационных технологий в защищенном исполнении;
- организация защищенного электронного документооборота, с использованием СКЗИ, развертывания системы удостоверяющих центров, применения электронной цифровой подписи и частных виртуальных сетей обмена информации по телекоммуникационным системам связи;
- разработка соответствующей ведомственной нормативно — правовой базы в области обеспечения информационной безопасности;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- развитие системы сертификации средств информатизации, программных продуктов, применения сертифицированных средств защиты информации и использование системы лицензирования деятельности в области защиты информации и международного информационного обмена;
- определение оптимального с экономической точки зрения отнесения информации к категории ограниченного доступа, в том числе государственной тайне и конфиденциальной информации;
- создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями пользователей (исполнителей работ) на объектах информатизации;

- подготовка кадров в области защиты информации.

Для достижения основных целей защиты *КСЗИ НСД на объектах информатизации* должна обеспечивать решение следующих основных задач:

- защиту от вмешательства в процесс функционирования ОИ посторонних лиц (возможность использования ОИ и доступа к ресурсам должны иметь только зарегистрированные установленным порядком пользователи или должностные лица);
- разграничение доступа зарегистрированных пользователей (в том числе внешних пользователей, пользователей из числа сотрудников взаимодействующих органов государственной власти, подведомственных предприятий, организаций и учреждений министерств и ведомств) к аппаратным, программным и информационным ресурсам ОИ (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), т.е. защиту от несанкционированного доступа;
- регистрацию действий пользователей при использовании защищаемых ресурсов на ОИ в системных журналах СЗИ от НСД и периодический контроль корректности действий пользователей путем анализа содержимого этих журналов специалистами по защите информации;
- контроль целостности (обеспечение неизменности) среды исполнения программ и её восстановление в случае нарушения;
- защиту от несанкционированной модификации и контроль целостности используемых на ОИ программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации от утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию в целях её уничтожения, искажения и блокирования и по противодействию техническим средствам разведки;
- 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.

Политика информационной безопасности

В разделе изложена политика информационной безопасности системы.

Цели политики информационной безопасности

Основными целями политики информационной безопасности является:

- обеспечение сохранности, целостности информационных ресурсов и предоставление доступа к ним в строгом соответствии с установленными приоритетами и правилами разграничения доступа;
- обеспечение защиты подсистем, задач и технологических процессов, от угроз информационной безопасности, описанных выше в настоящем документе;
- обеспечение защиты управляющей информации от угроз информационной безопасности, описанных выше в настоящем документе;
- обеспечение защиты каналов связи от угроз со стороны каналов связи.

Основой создания подсистемы информационной безопасности (ПИБ) является **политика информационной безопасности**, под которой понимается набор правил и практических рекомендаций, на которых строится обеспечение информационной безопасности, управление и распределение средств защиты информации на объектах информатизации.

Политика информационной безопасности должна представлять совокупность требований, правил, положений и принятых решений, определяющих:

- порядок доступа к информационным ресурсам;
- необходимый уровень (класс и категорию) защищенности объектов информатизации;
- организацию защиты информации в целом;

- дополнительные требования по защите отдельных компонент;
- основные направления и способы защиты информации.

Политика информационной безопасности направлена на обеспечение:

- *конфиденциальности (секретности) информации*, циркулирующей в системе, субъективно определяемой характеристике информации, указывающей на необходимость введения ограничений на круг субъектов информационных отношений, имеющих доступ к данной информации, и обеспечиваемую способность среды обработки сохранять информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;
- *целостности информации и среды её обработки*, то есть предотвращение несанкционированной модификации, реконфигурации или уничтожения информации, программных средств её обработки, а также предотвращения несанкционированного изменения структуры и её объектов информатизации;
- *доступности информации,* то есть способности информационной среды, средств и технологий обработки информации обеспечить санкционированный доступ субъектов к информации, программным и аппаратным средствам.

Защите подлежит принимаемая/передаваемая, обрабатываемая и хранимая информация содержащая:

- сведения, предназначенные для предоставления средствам массовой информации;
- иные сведения, не составляющую служебную тайну;
- сведения о частной жизни граждан (персональные данные), доступ к которым ограничен законодательством.

Обеспечение защиты открытой информации осуществляется организационными мерами, средствами сетевого и телекоммуникационного оборудования, а также стандартными средствами общего программного обеспечения (операционных систем, СУБД).

Первым шагом на пути обеспечения информационной безопасности является разработка политики информационной безопасности.

Принципы, реализуемые при построении подсистемы информационной безопасности

Подсистема информационной безопасности строится на базе использования следующих основных принципов:

- законность;
- системность;
- комплексность;
- непрерывность защиты;
- катастрофоустойчивость;
- равнопрочность;
- своевременность;
- использование существующей базы;
- использование серийных решений;
- преемственность и непрерывность совершенствования;
- преимущественное использование отечественных аппаратно-программных средств защиты;
- устойчивость функционирования средств защиты при отдельных отказах;
- масштабируемость подсистемы информационной безопасности;
- разумная достаточность;
- рубежность;
- разделение на подсистемы;
- персональная ответственность;
- минимизация полномочий;
- персонификация при определении порядка доступа к защищаемой информации;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;

- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- максимально возможная степень автоматизации процессов управления безопасностью;
- специализация и профессионализм;
- обязательность контроля;
- этапность.

Законность

Разработка подсистемы информационной безопасности при доступе к системе осуществляется в соответствии с действующим законодательством в области информации, информатизации и защиты информации, других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Принятые меры безопасности информации не должны препятствовать доступу к данным сотрудникам Организации в пределах своих полномочий в предусмотренных законодательством случаях к информации конкретных систем.

Системность

Системный подход к построению подсистемы информационной безопасности при доступе к системе предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых, для понимания и решения проблемы обеспечения безопасности информации АС ГЗК.

При создании подсистемы информационной безопасности учитываются 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 строится 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. Внешняя защита обеспечивается физическими средствами, организационными и правовыми мерами.

Кроме того, комплексный подход к обеспечению безопасности информации подразумевает использование защитных механизмов на всех этапах жизненного цикла системы, от её проектирования и до вывода из эксплуатации, и совместное решение целого спектра вопросов, начиная от физической защиты объектов АС ГЗК, с применением системы контроля доступа, и оканчивая вопросами поддержки функционирования в критических ситуациях.

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.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка, такая как обновление программного обеспечения, своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий. 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.
Кроме того, организационно-техническое обеспечение должно быть реализовано таким образом, чтобы при внесении любых изменений в структуру, адекватные изменения вносились и в её подсистеме защиты.

Катастрофоустойчивость

Означает такое построение и эксплуатацию, при которых вероятность безвозвратной потери информации, обрабатываемой и хранимой, при возможном разрушении, а также при возможном значительным или частичным нанесением физического ущерба зданиям, помещениям, в которых располагается оборудование и системам жизнеобеспечения, будет минимальна.

Равнопрочность

При создании системы комплексной защиты используется принцип равнопрочности защиты, при котором в системе отсутствуют элементы, снижающие уровень защищенности на отдельных её участках.

Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач ПИБ и реализацию мер обеспечения безопасности информации по мере развития системы в целом и её подсистемы информационной безопасности, в частности.

Использование существующей базы

Базой для подсистемы информационной безопасности является существующая система, находящаяся в процессе развития. При этом в подсистемы информационной безопасности максимально задействуются штатные механизмы защиты информации, имеющиеся в аппаратных и программных компонентах (на серверах, рабочих станциях, маршрутизаторах, в операционных системах, прикладном программном обеспечении).

Использование серийных решений

В системе комплексной защиты информации максимально используются серийно выпускаемое отечественное и зарубежное оборудование и программное обеспечение, адаптируемое к конкретным условиям эксплуатации и положительно себя зарекомендовавшее.

Преемственность и совершенствование

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

Преимущественное использование отечественных аппаратно-программных средств защиты

При построении ПИБ предполагается осуществить преимущественное использование отечественных аппаратно-программных средств защиты в рамках реализации единой политики информационной безопасности на объектах.

Устойчивость функционирования средств защиты

При проектировании ПИБ закладываются такие решения, которые бы обеспечили устойчивое функционирование средств защиты и доступ пользователей к ресурсам объектов, в условиях возможных отдельных отказов и сбоев оборудования и активных негативных воздействий на аппаратно-программные средства защиты.

Масштабируемость подсистемы информационной безопасности

Подсистема информационной безопасности должна удовлетворять требованию масштабируемости, то есть обеспечивать заданный уровень работоспособности и эффективности защиты в условиях динамического развития, роста объема информационных и программных ресурсов объектов.

Разумная достаточность

Предполагает экономическую целесообразность, сопоставимость возможного ущерба от разглашения, утраты, утечки, уничтожения и искажения информации и затрат на организацию её защиты. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы, в которой эта информация передается, обрабатывается и хранится. 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 возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности, заданный в РД Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации». Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Рубежностъ

Для каждой защищаемой системы используется принцип «рубежности» для построения многоуровневой системы доступа к защищаемой информации. Одним из эффективных внешних рубежей защиты системы должны быть СЗИ, реализованные на уровне операционных систем (ОС) в силу того, что ОС — это та часть компьютерной системы, которая управляет использованием всех её ресурсов. Рубеж защиты на прикладном уровне, учитывающий особенности предметной области, представляет собой внутренний рубеж защиты.

Уровни доступа к защищаемой информации

№ уровня защиты	**Наименование**
Уровень 5	Доступ к передаче информации по каналам связи (ввод ключа шифрования и ЭЦП)
Уровень 4	Доступ к информации в базах данных (ввод пароля в прикладном ПО для доступа к базам данных)
Уровень 3	Доступ к ресурсам (по аутентификации сетевого имени, ввод имени и индивидуального пароля для входа в сеть)
Уровень 2	Доступ к операционной системе рабочей станции (использование встроенных средств операционной системе)
Уровень 1	Система доступа в помещения (к рабочим станциям и оборудованию)
Уровень 0	Система доступа на объект информатизации

Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности информации и системы её обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников 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 сотруднику для выполнения его должностных обязанностей.

Принцип персонификации при определении порядка доступа к защищаемой информации

Означает, что все полномочия при определении порядка доступа пользователей и администраторов к защищаемой информации должны быть персональными, указаны явно и проверены непосредственно перед предоставлением доступа.

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 обладают определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установка средств защиты осуществляется 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 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 обеспечивается только за счет секретности структурной организации и алгоритмов функционирования её подсистем. Знание алгоритмов работы системы защиты не должно давать возможности её преодоления (даже авторам). Это однако не означает, что информация о конкретной системе защиты должна быть общедоступна.

Простота применения средств защиты

Механизмы защиты являются интуитивно понятными и простыми в использовании. Применение средств защиты не связывается со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не требует от пользователя выполнения рутинных малопонятных ему операций.

Научная обоснованность и техническая реализуемость

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

Максимально возможная степень автоматизации процессов управления безопасностью

При проектировании, эксплуатации ПИБ должна быть обеспечена максимально возможная степень автоматизации управления безопасностью информацией, в том числе и при управлении конфигурацией ПИБ.

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. Реализация административных мер и эксплуатация средств защиты должна осуществляется профессионально подготовленными специалистами Организации (специалистами подразделений технической защиты информации).

Обязательность контроля

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

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты осуществляется на основе применения средств

оперативного контроля и регистрации и охватывает как несанкционированные, так и санкционированные действия пользователей.

Этапность

Построение подсистемы информационной безопасности осуществляется поэтапно.

Приоритеты обеспечения информационной безопасности

С точки зрения требований к обеспечению информационной безопасности, обрабатывается информация следующих видов — открытая информация, конфиденциальная (служебная) информация.

Каждому виду информации соответствуют свои приоритеты в обеспечении информационной безопасности.

Для обеспечения работы пользователей с открытой информацией, при выполнении ими своих служебных обязанностей, определены следующие приоритеты в обеспечении информационной безопасности:

- целостность.
- доступность.

Для обеспечения работы пользователей с конфиденциальной (служебной) информацией, содержащей сведения ограниченного распространения, определены следующие приоритеты в обеспечении информационной безопасности:

- целостность;
- конфиденциальность;
- доступность.

Здесь:

- под **целостностью информации** понимается свойство автоматизированной системы сохранять неизменность или обнаруживать факт изменения информации и в последующем восстанавливать её, в условиях случайных и преднамеренных угроз, негативных воздействий, помех, ошибок, сбоев;
- под **конфиденциальностью информации** понимается свойство автоматизированной системы, заключающееся в том, что в условиях случайных и преднамеренных угроз информация предоставляется только авторизованному пользователю;
- под **доступностью информации** понимается свойство автоматизированной системы, заключающееся в том, что в условиях случайных и преднамеренных угроз информация предоставляется в том виде и том месте, которые необходимы авторизованному (санкционированному) пользователю, и в то время, когда она ему необходима. Доступность определяется как наличием необходимой информации, так и готовностью системы к обслуживанию.

Целостность информационных, вычислительных и телекоммуникационных ресурсов должна обеспечиваться и контролироваться с помощью специальных методов и средств защиты информации от несанкционированного доступа (НСД).

Осуществление контроля правильности работы прикладного программного обеспечения на рабочих станциях, непосредственно взаимодействующих с сетевыми ресурсами должно осуществляться с применением средств активного аудита.

Целостность передаваемых сообщений должна обеспечиваться применением криптографических механизмов вычисления контрольных сумм (коды аутентификации, имитовставки, электронная цифровая подпись).

Кроме того, целостность информации должна обеспечиваться применением специальных средств защиты от разрушающих программных компонент и средств контроля целостности.

Обеспечение конфиденциальности информации должно осуществляться:

- на прикладном (абонентском) уровне с применением системы контроля доступа на объекты и в помещения
- применением средств шифрования на сетевом уровне (шифраторы пакетов различных сетевых протоколов, криптомаршрутизаторы) при непременном условии обеспечения

достаточно высоких эксплуатационных характеристик оборудования ПИБ (быстродействие, надежность, удаленное управление).

Обеспечение доступности информации обеспечивается соответствующими архитектурными и техническими решениями построения, в том числе архитектурными и техническими решениями ПИБ, а также применением специальных регламентов и средств, таких как регламенты и средства резервного копирования, средства обеспечения бесперебойного электропитания оборудования.

Основные направления обеспечения информационной безопасности

Исходя из указанных выше приоритетов, основными направлениями обеспечения информационной безопасности при работе пользователей с конфиденциальной (служебной) информацией, являются:

- контроль и управление доступом на объекты, в помещения, в контуры обработки информации;
- защита информации от несанкционированного доступа (НСД);
- защита от разрушающих программных компонент (РПК) и контроль целостности;
- защита информации при передаче по внешним (открытым) каналам связи;
- защита информации от утечки по техническим каналам;
- выявление и противодействие возможным атакам по каналам связи и техническим каналам;
- регистрация и учет работы аппаратно-программных средств и пользователей;
- контроль и управление доступом к ресурсам;
- поддержание доступности информации.

Контроль доступа на объекты и в помещения

Контроль доступа на объекты регламентируется общими правилами Организации. В частности, доступ к объектам и помещениям, в которых установлено серверное оборудование, осуществляется обученным и сертифицированным персоналом и ограничивается стандартными офисными средствами безопасности.

Защита информации от несанкционированного доступа

Данная подсистема защиты информации должна быть реализована на базе комплексного использования штатных средств и функций защиты, предоставляемых оборудованием и программным обеспечением (встроенными средствами защиты сетевых операционных систем и систем управления базами данных (СУБД)).

При построении защиты от НСД необходимо, по возможности, избегать дублирования многих функций, с тем, чтобы ПИБ не страдала избыточностью, что в конечном итоге скажется как на удобстве работы пользователей и их желании выполнять все предписания системы защиты, так и на управляемости самой ПИБ.

Защита информации от НСД также должна обеспечиваться:

- средствами межсетевого экранирования;
- средствами криптографической защиты информации;
- средствами управления, анализа и аудита ПИБ в рамках сетевых конфигураций.

Средства межсетевого экранирования

Средства межсетевого экранирования должны использоваться для подключения к открытым сетям и для развязки разноуровневых сетей внутри, в том числе сетей, обрабатывающих информацию с различным грифом секретности.

Концепция систем типа Firewall (брандмауер, межсетевой экран) была разработана для снижения риска нелегального доступа к закрытой информации при подключении частных сетей (в том числе ЛВС} к сетям общего пользования.

Межсетевой экран представляет собой программно-аппаратный комплекс, размещенный на стыке двух сетей и реализующий следующие три функции:

- обеспечение обмена данными между сетями только через указанную систему;
- фильтрация трафика обмена;
- предотвращение возможности проникновения в сам экран.

В этом случае обеспечивается эффективная блокировка внешнего трафика частной сети и жесткий контроль за ним.

Кроме того, межсетевые экраны могут осуществлять разграничение доступа между различными сегментами одной корпоративной сети, а также контроль за информационными потоками, направленными во вне, обеспечивая тем самым необходимый режим конфиденциальности.

Применение межсетевых экранов также позволяет существенно уменьшить уязвимость внутренних сервисов безопасности, так как нарушителю необходимо вначале преодолеть защитные механизмы самого экрана, где они сконфигурированы особенно тщательно.

Однако лишь некоторые межсетевые экраны могут быть отнесены только к одной из указанных категорий.

В ПИБ, исходя из принципа «разумной достаточности», рекомендуется применять межсетевые экраны, реализующие функции первых трех типов, из указанных выше типов межсетевых экранов.

Средства криптографической защиты информации

Одним из приоритетных направлений обеспечения информационной безопасности является использование криптографических средств защиты информации (СКЗИ), в том числе криптомаршрутизаторов, средств криптографической аутентификации и электронной цифровой подписи (ЭЦП). ЭЦП должна генерироваться и проверяться с использованием средств ПИБ.

Средства управления, анализа и аудита

Средства аудита занимают свое особое положение в ряду средств обеспечения безопасности информации, заключающееся в том, что все действия нарушителя по преодолению средств защиты фиксируются, позволяя тем самым вовремя обнаружить попытку несанкционированного входа. Причем, учитывая принцип многоуровневой защиты, нарушителю придется преодолевать несколько защитных рубежей, что будет обязательно отмечено в регистрационном протоколе. В случае если указанная процедура выполняется в режиме реального времени, администратором безопасности могут быть своевременно предприняты соответствующие меры по предотвращению незаконного вторжения на одном из следующих уровнях защиты.

Кроме средств аудита часть программных продуктов также позволяет осуществлять оценку системы безопасности сети, имитируя известные способы, применяемые нарушителями для проникновения в интрасети, и тем самым, обнаруживая в системе защиты слабые места. Данные программные продукты не только выявляют уязвимые места, но и определяют действия, которые необходимо предпринять для ликвидации пробелов в сетевой системе безопасности. Администратору остается лишь выбрать способы их устранения.

Удостоверяющий центр

Для ведения B2B и B2G проектов необходимо провести развертывание Удостоверяющего центра (УЦ). УЦ должен обеспечить выполнение следующих основных функций:

- осуществление общего технического функционирования защищенного электронного документооборота при использовании СКЗИ;
- заключение договоров на установку и подключение программно-технических средств Пользователей;
- изготовление сертификатов открытых ключей подписей;
- регистрацию владельцев сертификатов открытых ключей подписей (Пользователей);
- ведение реестров Пользователей;
- выдачу Пользователям инсталляционных носителей информации с эталонным программным обеспечением СКЗИ и необходимой эксплуатационной документацией;
- обеспечение свободного доступа к реестру Пользователей;
- эффективное, надежное функционирование и непрерывный режим эксплуатации в рабочее время;

- поддержку основных средств сетевого взаимодействия, средств контроля, настройки и администрирования;
- взаимодействие с сетью удалённых Центров регистрации и ведение баз данных, содержащих информацию о владельцах сертификатов;
- организацию консультаций Пользователей по использованию криптографических средств защиты информации.

Для взаимодействия с удостоверяющими центрами, входящими в систему удостоверяющих центров Российской Федерации ведомственный УЦ должен обеспечивать возможность *кросс-сертификации*.

Для всех пользователей УЦ должен быть разработан и предоставлен документ «Сборник руководящих документов по организации системы защищенного электронного документооборота с использованием средств криптографической защиты информации в системе».

Для разрешения возникающих конфликтных ситуаций (разногласий) между пользователями защищенной сети разногласия разрешаются на ведомственном уровне.

Используемые СКЗИ в УЦ должны соответствовать требованиям ГОСТ 28147-89, Р34.10-94, Р34.11-94, Р 34.11-2001 и иметь сертификат ФСБ (ФАПСИ) на аппаратно-программное средство криптографической защиты информации (СКЗИ) по классу защищенности КС1.

Средства защиты от разрушающих программных компонент и контроля целостности

Учитывая, что в настоящее время среди отнесенных к специальным программам, содержащим в себе некие деструктивные элементы — разрушающие программные компоненты, массовое распространение получили компьютерные вирусы, особую актуальность приобретает использование антивирусных средств (АВС) защиты информации, предназначенных для работы в гетерогенных сетях.

В связи с этим в данном разделе описывается подход по осуществлению антивирусной защиты.

Для обеспечения надежной антивирусной защиты в состав ПИБ рекомендуется включить средства антивирусной защиты от двух независимых производителей.

Кроме того, имеется необходимость применения антивирусного сканера, предназначенного для осуществления проверки наличия вирусов в файлах, загружаемых программами просмотра (WEB-броузерами), а также в получаемых почтовых сообщениях, действуя совершенно прозрачно для пользователей.

Система защиты от вирусов ПИБ должна строиться исходя из обязательного выполнения следующих процедур:

- входной контроль новых программных средств и входной контроль поступающей по сети информации и данных (выполняется применяемыми АВС);
- защиту операционной системы и системных программ от заражения;
- карантинный режим эксплуатации нового программного обеспечения;
- резервирование главной загрузочной записи (MBR), таблицы размещения файлов и CMOS-памяти.

Организационные мероприятия по антивирусной защите также играют важную роль.

При их проведении необходимо учитывать, что для надежного функционирования системы антивирусной защиты конечные пользователи должны знать, какое программное обеспечение работает на каждой рабочей станции, а администратор безопасности — в том числе и на сервере, и ежесуточно проверять его целостность.

В целях успешной борьбы с компьютерными вирусами в рамках ПИБ должен быть спланирован и скоординирован подход для ликвидации вирусного заражения или атаки.

В рамках ПИБ должен вестись непрерывный контроль целостности ПО и данных. Обеспечение целостности ПО и данных имеет важное значение, и ввиду того, что для баз данных и для системы в целом, вероятно наиболее распространенными «нарушителями» являются ошибки оборудования, программ, администраторов и пользователей системы.

Под контролем целостности в общем плане понимается:

- проверка наличия в штатном комплекте ПО полной совокупности критичных по безопасности программных компонентов;
- проверка совпадения размеров ХЕШ-функций компонентов ПО и данных используемых при эксплуатации в штатном режиме с эталонными значениями этих компонентов, хранящимися в Архиве ХЕШ-Эталонов.

В рамках ПИБ контроль целостности ПО и данных, рекомендуется обеспечивать средствами общего программного обеспечения (операционных систем и СУБД).

Средства поддержания доступности информации

Средства резервного копирования

Резервное копирование программ и данных необходимо проводить с целью минимизации потерь в случае отказов оборудования, либо сбоев в программном обеспечении. Данная задача наиболее сложна именно в интрасетях с их распределенными ресурсами и неоднородностью, в которых работают компьютеры под управлением различных операционных систем. Учитывая клиент/серверный характер интрасетей функцию резервного копирования целесообразно выделить в виде отдельного сервера (сервера Backup).

Распространение клиент/серверного подхода на процедуру резервного копирования информации и данных имеет ряд преимуществ по сравнению с традиционными методами. Они выражаются в следующем:

- Администраторы рабочих групп освобождаются от необходимости согласования действий и самой процедуры создания локальных резервных копий.
- Единообразие процедуры создания резервных копий.
- Возможность мониторинга процесса резервирования и диагностики возникших проблем.

Одним из способов обеспечения высокой доступности информации является создание резервных копий с возможностью её хранения в двух местах: один экземпляр хранится поблизости от оригинала, а другой в удаленном безопасном месте.

Средства обеспечения бесперебойного питания

Безопасность приема/передачи, обработки и хранения информации, в немалой степени зависит от стабильности характеристик питающего напряжения.

В качестве объекта защиты выступает такое оборудование, как серверы, мосты, маршрутизаторы, концентраторы, то есть те устройства, где необходимо корректно завершить работу по обработке информации без потери каких-либо данных прежде, чем прекратится подача электропитания.

Для обеспечения бесперебойного питания, как правило, применяется распределенная система бесперебойного питания, используемая там, где необходимо подавать питание на отдельные устройства вычислительной сети.

Структура управления подсистемой информационной безопасности

Реализуется следующая организационная структура управления подсистемой обеспечения информационной безопасности при доступе к системе:

Первый уровень управления: постоянно действующая техническая комиссия (ПДТК), на которой рассматриваются вопросы разработки подсистемы информационной безопасности. Контроль за разработкой ПИБ осуществляют департаменты Организации в пределах своей компетенции.

Второй уровень управления: специализированные подразделения, группы специалистов или отдельные специалисты по защите информации, в органах, учреждениях и предприятиях Организации.

Обеспечение информационной безопасности организует департамент Информационных технологий, обеспечивая выполнение следующих основных функций в интересах разработки ПИБ:

- разработка проектов нормативных документов по обеспечению информационной безопасности;

- разработка рекомендаций по защите информации от НСД;
- анализ и выявление возможных внешних и внутренних угроз безопасности, возможных каналов утечки информации;
- разработка рекомендаций, выбор и проверка на совместимость с общим и технологическим программным обеспечением современных сертифицированных систем и средств (программных, программно-аппаратных, технических, криптографических и т.п.) защиты информации на испытательном стенде;
- разработка и поставка на объекты информатизации программно-технических комплексов в защищенном исполнении, предназначенных для обработки секретной информации;
- проведение специальных объектовых исследований средств вычислительной техники от утечки информации по каналу побочных электромагнитных излучений и наводок;
- организация проведения защитных мероприятий для выделенных помещений;
- разработка предложений и рекомендаций по защите конфиденциальной информации, в том числе в части использования криптографических средств защиты информации и при передаче информации по телекоммуникационным сетям связи;
- подготовка предложений и участие в развертывании VPN —сети, системы удостоверяющих центров и по применению электронной цифровой подписи;
- организация проведения подготовки и аттестации и контроля объектов информатизации по требованиям информационной безопасности;
- координация и участие в разработке защищенных информационных технологий и ГИС-технологий, с последующей их подготовкой к сертификации по требованиям безопасности информации;
- взаимодействие с подразделениями по защите информации в министерствах, службах и агентствах, с предприятиями, организациями, сертификационными лабораториями и аттестационными центрами по вопросам информационной безопасности;
- разработка предложений по совершенствованию защиты секретной информации, в том числе от её утечки по техническим каналам;
- оказание консультативной и практической помощи по защите государственной тайны и конфиденциальной информации на объектах информатизации;
- участие в установке и отладке сертифицированных средств и систем защиты информации на объектах информатизации;
- организация специализированных курсов, проведение подготовки и обучение, специалистов по защите информации, для объектов информатизации.

Внедрение и реализацию требований по обеспечению информационной безопасности на объектах информатизации в органах, учреждениях предприятиях и организациях осуществляют специально подготовленные специалисты, группы или специальные, структурные подразделения по защите информации.

Организационные методы обеспечения информационной безопасности

Основным методом обеспечения информационной безопасности является принятие организационных мер и регламентов, а также культуры орагнизации. Сотрудники Организации несут личную ответственность за обеспечение информационной безопасности Организации, в том числе:

- свою информированность в вопросах информационной безопасности;
- свои действия, которые несут угрозы информационной безопасности;
- свои действия, которые наносят ущерб информационной безопасности;
- халатное отношение к мерам обеспечения информационной безопасности.

Формирование политики информационной безопасности на объектах информатизации

Разработка и осуществление политики безопасности на объектах информатизации, соответствующей положениям законодательных актов и требованиям НД по защите информации, является необходимым условием обеспечения достаточного уровня защиты государственных и ведомственных информационных ресурсов.

Политика информационной безопасности на объектах информатизации определяет процедуры и правила достижения целей и решения задач информационной безопасности, детализирует, регламентирует эти правила (например):

- роли и обязанности должностных лиц, отвечающих за проведение политики информационной безопасности;
- определение прав доступа к информации ограниченного доступа (кто и при каких условиях может читать и модифицировать информацию).

На всех объектах информатизации должно быть разработано «Положение о разрешительной системе допуска и доступа пользователей к информационным и техническим ресурсам объекта информатизации», в котором устанавливается кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях, определяются правила разграничения доступа, которые предполагают определение для всех пользователей информационных и программных ресурсов, доступных им для конкретных операций (чтение, запись, модификация, удаление, выполнение) с помощью заданных программно-технических средств доступа.

Допуск пользователей к работе и информационным ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей должны производиться в соответствии с «Положением о разрешительной системе…» установленным порядком.

Все пользователи, допущенные к работе и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка автоматизированной обработки информации, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник должен подписывать соглашение-обязательство о не разглашении сведений доверенных ему, соблюдении и ответственности за нарушение установленных требований по сохранению государственной тайны и конфиденциальной информации, а также правил работы с защищаемой информацией.

Обработка защищаемой информации на ОИ должна производиться в соответствии с утвержденными технологическими инструкциями по обеспечению информационной безопасности (включая вопросы восстановления информации при сбоях и отказах техники и ПО, текущего копирования, резервирования и архивирования).

Распределение идентификаторов, имен, генерация паролей, сопровождение правил разграничения доступа к базам данных возлагается на администраторов конкретных баз данных и специалистов по защите информации. При этом могут использоваться как только штатные (сертифицированные), так и дополнительные средства защиты СУБД и операционных систем.

На этапе ввода в эксплуатацию объектов информатизации её пользователи, а также административный, руководящий и обслуживающий персонал должны быть ознакомлены с перечнем сведений, подлежащих засекречиванию, технологическими инструкциями (под роспись), в части их касающейся, и своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации ограниченного доступа.

Для непосредственной организации, эффективного функционирования и контроля КСЗИ НСД на ОИ, в зависимости от объема выполняемых работ, должна быть создана специальная служба обеспечения информационной безопасности или назначены специалисты по защите, прошедшие необходимое обучение.

Система разработки нормативных документов по защите информации

Система разработки нормативных документов по обеспечению информационной безопасности создается для достижения следующих целей:

- оснащения органов, учреждений и предприятий Организации необходимой НД в области обеспечения информационной безопасности, применительно и с учетом специфики создания объектов информатизации АС ГЗК, в части их касающейся;

- координации принимаемых решений в области обеспечения информационной безопасности, сокращения сроков и затрат за счет стандартизации, унификации и типизации применяемых (в основном сертифицированных) СЗИ, контроля эффективности и общесистемных решений;
- обеспечения повышения эффективности и согласованности процесса управления обеспечением информационной безопасностью для объектов информатизации различного уровня.

Система НД по обеспечению информационной безопасности строится на основе следующих основных принципов:

- комплексность охвата проблемы;
- иерархичность построения с разграничением сферы действия и статуса обязательности отдельных видов НД;
- непротиворечивость и взаимосогласованность документов различного уровня;
- оптимальность состава (количества) документов;
- обоснованность включаемых требований.

Разработка и оснащение необходимыми НД, на основании которых осуществляется комплекс мероприятий и работ по обеспечению информационной безопасности, организуется департаментом инфомрационных технологий Организации.

Разрабатываются НД, областью распространения которых является организация защиты:

- конфиденциальной информации (включающей информацию ограниченного распространения с пометкой «Для служебного пользования», персональные данные и коммерческую тайну);
- открытой информации (для защиты её целостности, сохранности и достоверности).

Необходимые НД разрабатываются в соответствии и с учетом требований действующего законодательства Российской Федерации в области защиты информации, руководящих документов ФСТЭК (Гостехкомиссии) России, ФСБ России и других министерств, служб и агентств и документации на системы и средства защиты информации.

Органы, учреждения и предприятия Организации руководствуются этими НД, на их основе разрабатывают свои методические и инструктивные документы (если это необходимо) или дополняют действующие документы, в части их касающейся, с учетом специфики функционирования объектов информатизации.

Источники и нормативные документы

В данном разделе приведены ссылки на нормативные и обзорные документы.

Нормативные документы

В данном разделе приведены ссылки на ГОСТы и руководящие документы, определяющие политику информационной безопасности.

1. Закон Российской Федерации «О государственной тайне» от 21.07.93 №5485
2. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.2006г. № 149-ФЗ; (ред. от 08.06.2020)
3. Закон Российской Федерации «О персональных данных» от 27.07.2006г. № 152-ФЗ.
4. Закон Российской Федерации «О сертификации продукции и услуг» от 10.06.93 №5151-1.
5. Закон Российской Федерации «О международном информационном обмене» от 04.07.96 №85-ФЗ.
6. «Доктрина информационной безопасности Российской Федерации», утверждена Президентом Российской Федерации 9.09.2000 г. № Пр.-1895.
7. Указ Президента Российской Федерации от 17.12.97 г. № 1300 «Концепция национальной безопасности Российской Федерации» в редакции указа Президента Российской Федерации от 10.01.2000 г. №24.
8. Указ Президента Российской Федерации от 06.03.97 г. № 188 «Перечень сведений конфиденциального характера».

9. Постановление Правительства Российской Федерации от 03.11.94 г. №1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органов исполнительной власти».
10. Указ Президента Российской Федерации «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30.11.95 №1203.
11. «Положение о государственном лицензировании деятельности в области защиты информации". Утверждено решением Гостехкомиссии и ФАПСИ при Президенте Российской Федерации от 27.04.94 №10.
12. Дополнения и изменения в «Положение о государственном лицензировании деятельности в области защиты информации». Решение Гостехкомиссии России и ФАПСИ от 24.06.97 №60.
13. «Положение о сертификации средств защиты информации». Утверждено постановлением Правительства Российской Федерации от 26.06.95 №608.
14. «Положение о сертификации средств защиты информации по требованиям безопасности информации». Зарегистрировано Госстандартом России в Государственном реестре 20.03.95. Введено в действие приказом Председателя Гостехкомиссии России от 27.10.95 с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26.06.95 №608.
15. «Положение по аттестации объектов информатизации по требованиям безопасности информации». Утверждено Председателем Гостехкомиссии России 25.11.94.
16. ГОСТ Р 50922-96 «Защита информации. Основные термины и определения».
17. ГОСТ 29339-92 «Информационная технология. Защита информации от утечки за счет ПЭМИН при её обработке средствами вычислительной техники. Общие технические требования».
18. ГОСТ Р 50752-95 «Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при её обработке средствами вычислительной техники. Методы испытаний».
19. ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положения».
20. ГОСТ 28195—89. «Оценка качества программных средств. Общие положения»;
21. ГОСТ Р 51583-2000 «Порядок создания автоматизированных систем в защищенном исполнении».
22. ГОСТ Р 51241-98 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».
23. ГОСТ Р ИСО 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель».
24. ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации».
25. ГОСТ 2.114- 95 «Единая система конструкторской документации. Технические условия».
26. ГОСТ 2.601- 95 «Единая система конструкторской документации. Эксплуатационные документы».
27. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».
28. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».
29. ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».
30. ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функции хэширования».

31. ГОСТ Р ИСО/МЭК 15408-1-2002. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».
32. ГОСТ Р ИСО/МЭК 15408-2-2002. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».
33. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности».
34. «Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (приказ Гостехкомиссии России от 19.06.2002г. № 187).
35. РД.50-492—84. «Методика оценки научно-технического уровня АСУ. Типовые положения».
36. РД.50-680—88. «Методические указания. Автоматизированные системы. Основные положения».
37. ГОСТ 34.602—89. «Информационная технология. Комплекс стандартов на АС. Техническое задание на создание автоматизированной системы».
38. РД.50-34.698—90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на АС. АС. Требования к содержанию документов».
39. ГОСТ 34.201—89. «Информационная технология. Комплекс стандартов на АС. Виды, комплектность и обозначение документов при создании АС».
40. ГОСТ 34.936—91. «Информационная технология. ЛВС. Определение услуг уровня управления доступом».
41. ГОСТ 24.104—85. «Автоматизированные системы управления. Общие требования».
42. ГОСТ 24.702—85. «Эффективность АСУ».
43. ГОСТ 24.703—85. «Типовые проекты решения АСУ».
44. ГОСТ 34.603—92. «Виды испытаний автоматизированных систем».
45. ГОСТ 26139—84. «Интерфейс для АСУ рассредоточенными объектами. Общие требования».
46. ГОСТ 16504—81. «Испытания и контроль качества продукции».
47. ГОСТ 29099—91. «Сети вычислительные локальные. Термины и определения.
48. «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)».
49. Руководящий документ «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». Гостехкомиссия России. Москва. Военное издательство. 1992г.
50. Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». Гостехкомиссия России. Москва. Военное издательство. 1992г.
51. Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Гостехкомиссия России. Москва. Военное издательство. 1992г.
52. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ». Гостехкомиссия России. Москва. Военное издательство. 1992г.
53. Руководящий документ «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации». Гостехкомиссия России. Москва. Военное издательство. 1992г.

54. РД «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей». Гостехкомиссия России Москва, 1999г.
55. Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации». Утвержден решением Председателя Гостехкомиссии России от 25.07.97.
56. «РД. Концепция обеспечения информационной безопасности в системе Государственного комитета Российской Федерации по земельной политике». (Госкомзем России, 2000г.).
57. «РД. Типовое Руководство по защите информации, составляющей государственную тайну, от технических разведок и от её утечки по техническим каналам в системе Госкомзема России». (Госкомзем России, 2000г.).
58. «РД. Временное типовое Положение по защите информации, составляющей государственную тайну, при её обработке в автоматизированных системах в системе Государственного комитета Российской Федерации по земельной политике». (Госкомзем России, 2000г.).
59. «РД. Временная Инструкция о порядке обращения и обеспечения защиты конфиденциальной информации при её обработке в системе Государственного комитета Российской Федерации по земельной политике». (Госкомзем России, 2000г.).
60. «РД. Типовая программа и методика проведения аттестационных испытаний автоматизированных систем на соответствие требованиям по безопасности информации в системе Государственного комитета Российской Федерации по земельной политике». (Госкомзем России, 2000г.).
61. Семейство международных стандартов ISO 27000, регламентирующих информационную безопасность.

Источники

В разделе приведены ссылки на справочники, описания стандартов и принципов построения политики информационной безопасности.

1. Политика информационной безопасности при доступе к сведениями государственного земельного кадастра.
2. Стандарты информационной безопасности.
3. Описание Health Insurance Portability and Accountability Act.
4. Описание Gramm–Leach–Bliley Act.
5. Описание Sarbanes–Oxley Act.
6. Описание Payment Card Industry Data Security Standard.
7. «Терминология в области информационной безопасности. Справочник по терминам, понятиям и определениям» (Госкомзем России, 2000г.).

Перечень сведений, отнесенных к коммерческой тайне

Следующий список содержит документы и сведения, составляющие коммерческую тайну Организации.

1. Бухгатерские документы.
2. Планы (бизнес, логистика) текущих проектов.
3. Переписка с заказчиками.
4. Учётные записи и пароли доступа к информации.