УТВЕРЖДАЮ
Главный врач АУЗРА «РСП»
_____ А.М. Белекова
«___» _____ 20__г.

АВТОНОМНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ АЛТАЙ «РЕСПУБЛИКАНСКАЯ СТОМАТОЛОГИЧЕСКАЯ ПОЛИКЛИНИКА»

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Содержание

1. Вводные положения

1. Введение

Настоящий Стандарт устанавливает Политики информационной безопасности (правила обеспечения информационной безопасности, порядок разработки и сопровождения информационных систем (ИС) автономного учреждения здравоохранения Республики Алтай «Республиканская стоматологическая поликлиника») и является основным документом, регламентирующим деятельность автономного учреждения здравоохранения Республики Алтай «Республиканская стоматологическая поликлиника» (далее - «Поликлиника») в области безопасности информационных технологий.

1.2. Цели

Настоящий Стандарт разработан с целью информирования пользователей, сотрудников и руководства Поликлиники о наложенных на них обязательных требованиях по защите информационных ресурсов.

1.3. Задачи

Задачами настоящего Стандарта являются:

- описание организации системы управления информационной безопасностью в Поликлинике;
- определение Политик информационной безопасности Поликлиники, а именно:
  - Политика реализации антивирусной защиты;
  - Политика учетных записей;
  - Политика предоставления доступа к информационному ресурсу;
  - Политика использования информационного ресурса в рамках существующих информационных систем;
  - Политика использования паролей;
  - Политика защиты АРМ;
  - Политика конфиденциального делопроизводства;
  - определение порядка сопровождения ИС Поликлиники.

1.4. Область действия

Настоящий Стандарт распространяется на все подразделения Поликлиники кроме тех, в которых ведется обработка сведений отнесенных к Государственной тайне.

Требования настоящего Стандарта распространяются на всех лиц, имеющих доступ к информации, принадлежащей Поликлинике, на основании своих должностных обязанностей или договорных отношений.

1.5. Период действия и порядок внесения изменений

Настоящий Стандарт вводится в действие Приказом – главного врача Поликлиники. Стандарт признается утратившим силу на основании Приказа – главного врача Поликлиники. Изменения в Стандарт вносятся Приказом – главного врача Поликлиники.

Инициаторами внесения изменений в Стандарт являются:

- Лицо ответственное за информационную безопасность;
- Прочие структурные подразделения Поликлиники.

Плановая актуализация настоящего Стандарта производится ежегодно.

Внеплановая актуализация настоящего Стандарта производится в обязательном порядке в следующих случаях:

- при внесении существенных изменений в типовую конфигурацию программно - аппаратных средств Поликлиники;
- при изменении политики РФ в области информационной безопасности, указов и законов РФ в области защиты информации;

при изменении категорий обрабатываемой информации в Поликлинике;
при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности Поликлиники;
при изменении условий эксплуатации ЛВС Поликлиники;
при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, влекущего ущерб Поликлинике.

ветственными за актуализацию настоящего Стандарта (плановую и внеплановую) г администратор информационной безопасности.
нтроль за исполнением требований настоящего Стандарта и поддержанием его в ном состоянии возлагается на администратора информационной безопасности.

2. Термины и определения

томатизированная система – система, состоящая из персонала и комплекса средств изации его деятельности, реализующая информационную технологию выполнения ленных функций.
министратор сети – сотрудник или группа сотрудников службы технической жки, осуществляющие непосредственную организацию и выполнение работ по созданию изации), техническому обслуживанию и управлению (администрированию) ационной управляющей ЛВС, включая технические аспекты информационной ности.
тентификация - проверка принадлежности субъекту доступа предъявленного им фикатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем пользователем своего пароля на клавиатуре компьютера.
утренняя сеть - внутренний участок корпоративной сети, отделенный от внешней сети Интернет) и DMZ межсетевым экраном. Внутренняя сеть объединяет производственные, ые, административные сети и сети разработчиков.
емилитаризованная зона (DMZ) - участок корпоративной сети, расположенный между им МЭ и внешним маршрутизатором, используемым для подключения корпоративной сети телекоммуникационных провайдеров (сети Интернет). В DMZ размещаются ы, используемые для взаимодействия и предоставления сетевых сервисов внешним вателям корпоративной сети, а также серверы, которые по соображениям мационной безопасности не целесообразно размещать во внутренней сети Поликлиники.
оступ к информации - возможность получения информации и ее использования.
оступность информации - состояние информации, характеризуемое способностью АС ечивать беспрепятственный доступ к информации субъектов имеющих на это полномочия.
ащищенный канал передачи данных - логические и физические каналы сетевого одействия, защищенные от прослушивания потенциальными злоумышленниками твами шифрования данных (средствами VPN), либо путем их физической изоляции и щения на охраняемой территории.
Идентификатор доступа – уникальный признак субъекта или объекта доступа.
Идентификация - присвоение субъектам доступа (пользователям, процессам) и объектам па (информационным ресурсам, устройствам) идентификатора и (или) сравнение являемого идентификатора с перечнем присвоенных идентификаторов.
Администратор информационной безопасности – сотрудник или группа сотрудников а информационных технологий, осуществляющие контроль за обеспечением защиты рмации в ЛВС, а также осуществляющие организацию работ по выявлению и упреждению возможных каналов утечки информации, потенциальных возможностей ествления НСД к защищаемой информации.
Информация – сведения (сообщения, данные) независимо от формы их представления.
Информационная безопасность – состояние защищенности информационной среды, печивающее ее формирование, использование и развитие в интересах Поликлиники.

Информационная среда – совокупность информационно-телекоммуникационной системы поликлиники, процессов, источников и потребителей информации, обслуживающего персонала и пользователей информационных систем, обеспечивающего автоматизацию производственных процессов Поликлиники.

Информационная система - совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения производственных задач подразделений Поликлиники. В Поликлинике используются различные типы информационных систем для решения производственных, управленческих, учетных и других задач.

Информационно-телекоммуникационная система – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники, а также информационные системы, обеспечивающие автоматизацию процессов Поликлиники, и средства защиты информации.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационные активы – информационные системы, информационные средства, информационные ресурсы.

Информационные средства – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий, используемая в производственных - процессах Поликлиники.

Инфраструктура открытых ключей (ИОК, PKI) – технологическая инфраструктура и сервисы, обеспечивающие безопасность информационных и коммуникационных систем на основе использования криптографических алгоритмов и сертификатов ключей подписей.

Конфиденциальная информация - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Корпоративная сеть - объединение информационных систем, компьютерного, телекоммуникационного и офисного оборудования всех подразделений, посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.

Критичная информация - информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений Поликлиники, привести к причинению Поликлиники материального или иного вида ущерба.

Криптопровайдер – программный или программно-аппаратный модуль, реализующий алгоритмы шифрования.

Локальная вычислительная сеть (ЛВС) - группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Межсетевой экран (МЭ) - программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав корпоративной сети, а также между корпоративной сетью и внешними сетями (сетью Интернет).

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Операционная система – системная программа, осуществляющая взаимодействие пользователя и прикладных программ с аппаратной частью ЭВМ.

Ответственное лицо (администратор) информационных активов – работник Поликлиники, получивший на основании соответствующего распорядительного документа права обладателя информации, обрабатываемой в информационной системе Примечание: Понятия "Ответственное лицо (администратор) информационных активов и "владелец информационных средств (ресурсов)" идентичны.

Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом.

Периметральное средство защиты информации (СЗИ) – шлюз информационной безопасности, обеспечивающий межсетевое экранирование и защиту данных пересылаемых по открытым каналам связи (шифрование), а так же фильтрацию вредоносного ПО и блокирование внешних атак.

Пользователь ЛВС – работник Поликлиники (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в корпоративной сети в установленном порядке и получивший права на доступ к ресурсам корпоративной сети в соответствии со своими функциональными обязанностями.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция - персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Регистрационная (учетная) запись пользователя - включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Сервер – выделенный компьютер, имеющий разделяемые ресурсы, выполняющий определенный перечень задач и предоставляющий пользователям ЛВС ряд сервисов.

Сетевые (информационные) сервисы - сетевые приложения, предоставляющие различные виды сервисов для внутренних и внешних пользователей корпоративной сети, включая DNS, FTP, HTTP, Telnet, и другие.

Список контроля доступа (ACL) - правила фильтрации сетевых пакетов, настраиваемые на маршрутизаторах и МЭ, определяющие критерии фильтрации и действия, производимые над пакетами.

Средства криптографической защиты информации – средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Удостоверяющий центр – автоматизированная система, включающая в себя аппаратно-программные средства, нормативно-методическую документацию и пользователей.

Узел – совокупность ЛВС Поликлиники, расположенных в пределах одной контролируемой зоны.

Целостность информации - состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

ЭВМ – электронная - вычислительная машина, персональный компьютер.

Электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца ключа подписи, а также установить отсутствие искажения информации в электронном документе.

VPN (VIRTUAL PRIVATE NETWORK) - "Виртуальная частная сеть": технология и организация систематической удаленной связи между выбранными группами узлов в крупных распределенных сетях.

Обозначения и сокращения

АРМ - Автоматизированное рабочее место.
АС - Автоматизированная система.
БД - База данных.
ЗИ - Защита информации.
ИБ - Информационная безопасность.
ИОК - Инфраструктура открытых ключей.
ИС - Информационная система.
ИТС - Информационно-телекоммуникационная система.
КЗ - Контролируемая зона.
МЭ - Межсетевой экран.
НСД - Несанкционированный доступ.
ОС - Операционная система.
ПБ – Политики безопасности.
ПО - Программное обеспечение.
СВТ - Средства вычислительной техники.
СЗИ - Средство защиты информации.
СКЗИ - Средство криптографической защиты информации.
СПД - Система передачи данных.
СУБД - Система управления базами данных.
СУИБ - Система управления информационной безопасностью.
СЭД - Система электронного документооборота.
ЭВМ – электронная - вычислительная машина, персональный компьютер.
ЭЦП - Электронная цифровая подпись.

3. Политики информационной безопасности Поликлиники

3.1. Назначение политик информационной безопасности

Политики информационной безопасности Поликлиники – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в Поликлинике.

Под политиками безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политики информационной безопасности относятся к административным мерам обеспечения информационной безопасности и определяют стратегию Поликлиники в области ИБ.

Политики информационной безопасности (далее, ПБ) регламентируют эффективную работу средств защиты информации. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политики информационной безопасности реализуются посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политики, должны быть утверждены главным врачом Поликлиники.

3.2. Соответствие ПБ действующему законодательству

Правовую основу Политик составляют Конституция Российской Федерации, законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, Поликлиники и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

3.3. Ответственность за реализацию политик информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт администратор информационной безопасности.

Ответственность за реализацию Политик возлагается:

- в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на администратора информационной безопасности;
- в части, касающейся доведения правил Политик до сотрудников Поликлиники, а также иных лиц (см. область действия настоящего Стандарта) – на администратора информационной безопасности, а также руководителей структурных подразделений Поликлиники;
- в части, касающейся исполнения правил Политики, – на каждого сотрудника Поликлиники, согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящего Стандарта.

3.4. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация просвещения сотрудников Поликлиники в области информационной безопасности возлагается на руководителей подразделений и администратора информационной безопасности. Обучение работников Поликлиники правилам обращения с конфиденциальной информацией, проводится путем:

- проведения администратором информационной безопасности инструктивных занятий с работниками, принимаемыми на работу в Поликлиники;

– самостоятельного изучения работниками внутренних нормативных документов Поликлиники, регламентирующих вопросы защиты информации.

Допуск персонала к работе с информационными ресурсами Поликлиники осуществляется только после его ознакомления с настоящими Политиками, а также после ознакомления пользователей с "Инструкцией по работе пользователей в АС Автономного учреждения здравоохранения Республики Алтай «Республиканская стоматологическая поликлиника»", а так же иными инструкциями пользователей отдельных информационных систем. Согласие на соблюдение правил и требований настоящих Политик подтверждается подписями сотрудников в специальном журнале (бланке).

Допуск персонала к работе с конфиденциальной информацией Поликлиники осуществляется согласно соответствующих списков и инструкций. Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками Поликлиники, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

3.5. Защищаемые информационные ресурсы Поликлиники

Различаются следующие категории информационных ресурсов, подлежащих защите в Поликлиники:

Конфиденциальная - информация, определенная в соответствии с Федеральным Законом от 27.07.2006г. №149-ФЗ "Об информации, информационных технологиях и о защите информации", ФЗ от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне», ФЗ от 27.07.2006 г. №152-ФЗ "О персональных данных", указом президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера», постановлением правительства РФ от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», предусмотренная Перечнем сведений ограниченного распространения.

Публичная - информация, получаемая из публичных источников (публикации в СМИ, теле и радиовещание и т.д.). Информация, предназначенная для размещения на внешних публичных ресурсах;

Открытая - информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят. Информация, сформированная в результате деятельности Поликлиники, которую запрещено относить конфиденциальной на основании законодательства России. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности Поликлиники или имеющая принципиальное значение для развития Поликлиники;

Ограниченного доступа - информация, не попадающая под остальные категории, доступ к которой должен быть ограничен определенной категории лиц.

Конфиденциальная информация представляет собой сведения ограниченного доступа, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

Конфиденциальность документов определяется по наличию сведений установленных в "Перечне сведений конфиденциального характера".

Подходы к решению проблемы защиты информации в Поликлинике, в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования производственных процессов Поликлиники.

Для этого в Поликлинике выполняются следующие мероприятия:

– определяется порядок работы с документами, образцами изделиями и др., содержащими конфиденциальные сведения;
– устанавливается круг лиц и порядок доступа к подобной информации;

- вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные сведения;
- включаются в трудовые договоры с сотрудниками обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

Форма подписки о неразглашении конфиденциальной информации подписывается при инструктаже по информационной безопасности, если данное лицо/должность в силу своих должностных обязанностей будет иметь дело с конфиденциальной информацией. Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых Поликлиники с другими организациями. Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Согласно Ст.86 п.7 Трудового кодекса РФ защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

Согласно Ст.88 Трудового кодекса РФ при передаче персональных данных работника работодатель должен соблюдать следующие требования:

- осуществлять передачу персональных данных работника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым работник должен быть ознакомлен под расписку;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций.

Согласно Ст.90 Трудового кодекса РФ лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

3.6. Организация системы управления информационной безопасностью Поликлиники

3.6.1. Организация системы управления ИБ

Система управления информационной безопасности Поликлиники (СУИБ) – предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности Поликлиники.

Для успешного функционирования СУИБ Поликлиники должны быть реализованы следующие процессы:

- определение и уточнение области действия СУИБ и выбор подхода к оценке рисков ИБ;
- определение и уточнение области действия СУИБ должно осуществляться на основе результатов оценки рисков, связанных с основной деятельностью Поликлиники, а также оценки репутационных и правовых рисков деятельности Поликлиники;
- анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов и производственных – процессов;
- выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ;
- принятие руководством Поликлиники остаточных рисков и решения о реализации и эксплуатации/совершенствовании СУИБ. Остаточные риски ИБ должны быть соотнесены с рисками деятельности Поликлиники и оценено их влияние на достижение целей деятельности Поликлиники.

6.2. Реализация системы управления ИБ

В системе управления ИБ должны быть реализованы следующие процессы:

- разработка плана обработки рисков ИБ;
- реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СУИБ;
- реализация программ по обучению и осведомленности ИБ;
- обнаружение и реагирование на инциденты безопасности;
- обеспечение непрерывности деятельности и восстановления после прерываний.

На этапе планирования определяется политика и методология управления рисками, а также полняется оценка рисков, включающая в себя инвентаризацию активов, составление офилей угроз и уязвимостей, оценку эффективности контрмер и потенциального ущерба, ределение допустимого уровня остаточных рисков.

На этапе реализации производится обработка рисков и внедрение механизмов контроля, едназначенных для их минимизации. Руководством Поликлиники принимается одно из тырех решений по каждому идентифицированному риску: проигнорировать, избежать, редать внешней стороне, либо минимизировать. После этого разрабатывается и внедряется ан обработки рисков.

На этапе проверки отслеживается функционирование механизмов контроля, нтролируются изменения факторов риска (активов, угроз, уязвимостей), проводятся аудиты и полняются различные контролирующие процедуры.

На этапе действия по результатам непрерывного мониторинга и проводимых проверок, полняются необходимые корректирующие действия, которые могут включать в себя, в стности, переоценку величины рисков, корректировку политики и методологии управления сками, а также плана обработки рисков.

6.3. Методы оценивания информационных рисков

Оценка информационных рисков Поликлиники выполняется по следующим основным апам:

- идентификация и количественная оценка информационных ресурсов, значимых для работы Поликлиники;
- оценивание возможных угроз;
- оценивание существующих уязвимостей;
- оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые для производственного процесса уязвимые формационные ресурсы Поликлиники подвергаются риску, если по отношению к ним ществуют какие-либо угрозы.

ри этом информационные риски зависят от:

- показателей ценности информационных ресурсов;
- вероятности реализации угроз для ресурсов;
- эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной формационной системы и ее ресурсов. В результате оценки рисков становится возможным брать средства, обеспечивающие желаемый уровень информационной безопасности рганизации.

При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, ффективность существующих и планируемых средств защиты. Сами показатели ресурсов, начимости угроз и уязвимостей, эффективность средств защиты могут быть определены как олличественными методами, например, при определении стоимостных характеристик, так и чественными, например учитывающими штатные или чрезвычайно опасные нештатные здействия внешней среды.

Возможность реализации угрозы оценивается вероятностью ее реализации в течение заданного отрезка времени для некоторого ресурса Поликлиники.

При этом вероятность того, что угроза реализуется, определяется следующими основными показателями:

- привлекательностью ресурса, используется при рассмотрении угрозы от умышленного воздействия со стороны человека;
- возможностью использования ресурса для получения дохода, также используется при рассмотрении угрозы от умышленного воздействия со стороны человека;
- техническими возможностями реализации угрозы, используется при умышленном воздействии со стороны человека;
- степенью легкости, с которой уязвимость может быть использована.

3.7. Политики информационной безопасности

3.7.1. Политика предоставления доступа к информационному ресурсу

3.7.1.1. Назначение

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к информационным ресурсам Поликлиники.

3.7.1.2. Положение политики

К работе с информационным ресурсом допускаются пользователи, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящей Политикой.

Каждому сотруднику Поликлиники, допущенному к работе с конкретным информационным ресурсом Поликлиники, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться, и работать в ИС.

В случае производственной необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в Поликлинике одного и того же имени пользователя ("группового имени") ЗАПРЕЩЕНО.

3.7.1.3. Порядок создания (продления) учетной записи пользователя

Процедура регистрации (создания учетной записи), так же продления срока действия временной учетной записи пользователя для сотрудника Поликлиники инициируется заявкой сотрудника (Приложение № 1).

В заявке указывается:

- должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
- основание для регистрации учетной записи (номер приказа о принятии на работу в Стоматологическую поликлинику или иного договорного документа, определяющего необходимость предоставления работнику доступа к информационным ресурсам Поликлиники).

Заявку подписывает специалист отдела кадров, тем самым подтверждающий, что указанный работник действительно принят в штат Поликлиники (для работников не входящих в штат Поликлиники – руководитель курирующего соответствующие договорные отношения), утверждая тем самым производственную необходимость регистрации данного сотрудника в ИС Поликлиники.

Администратор информационной безопасности рассматривает представленную заявку и исполняет ее или передает для исполнения сервисной организации, осуществляющей администрирование ИС Поликлиники.

На основании заявки (задания) сотрудники совершают необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения

роля и минимальных прав доступа к сетевым ресурсам Поликлиники, таких как право гистрации на АРМ работника и пользования корпоративной электронной почтой.

По окончании регистрации учетной записи пользователя в заявке делается отметка о полнении задания за подписями исполнителей.

Минимальные права в Поликлинике, определенные выше, а также присвоение начального роля производится лицом ответственным за информационную безопасность при согласовании вки на предоставление (изменение) прав доступа пользователя к информационным ресурсам.

7.1.4. Порядок предоставления (изменения) полномочий пользователя

Процедура предоставления (или изменения) прав доступа пользователя к ресурсам диклиники инициируется заявкой сотрудника (Приложение № 2).

В заявке указывается:

- должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- наименование информационного актива (системы, ресурса), к которому необходим допуск (или изменение полномочий пользователя);
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач на конкретных информационных ресурсах ИС) с указанием разрешенных видов доступа к ресурсу (ролей).

Заявку подписывает специалист отдела кадров Поликлиники тем самым подтверждающий, указанный работник действительно принят в штат Поликлиники (для работников не дящих в штат Поликлиники – руководитель курирующего соответствующие договорные ошения), утверждая тем самым производственную необходимость допуска (изменения прав тупа) данного сотрудника к необходимым для решения им указанных задач ресурсам ИС виклиники и согласуется с владельцем (администратором) информационного актива.

Администратор информационной безопасности рассматривает представленную заявку и сят необходимые изменения в списки полномочий пользователей соответствующих формационных ресурсов.

По окончании внесения изменений в заявке делается отметка о выполнении задания за писями исполнителей.

.1.5. Порядок удаления учетной записи пользователя

При наступлении момента прекращения срока действия полномочий пользователя ончание договорных отношений, увольнение работника) учетная запись должна немедленно кироваться.

Предпочтительно использовать механизмы автоматического блокирования учетных исей уволенных работников, используя соответствующие ИС. При невозможности оматического блокирования учетных записей, работникам сопоставляются временные тные записи (с фиксированным сроком действия), о чем делается отметка в заявке при ее олнении и в обязательном порядке доводится до инициатора заявки.

Допускается регистрация постоянных учетных записей при отсутствии механизмов оматической блокировки. В этом случае специалисту отдела кадров Поликлиники (для отников не входящих в штат Поликлиники – руководителям курирующего соответствующие оворные отношения) вменяется в обязанность своевременно подавать заявки на кирование учетной записи работника не позднее, чем за сутки до момента прекращения ка действия полномочий пользователя.

В заявке указывается:

- должность работника (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;

– дата прекращения полномочий пользователя.

Заявку подписывает специалист отдела кадров (для работников не входящих в штат ликлиники – руководитель структурного подразделения курирующего соответствующие говорные отношения), утверждая тем самым факт прекращения срока действия полномочий льзователя.

Администратор информационной безопасности рассматривает представленную заявку и оизводят блокировку учетной записи пользователя.

По окончании внесения изменений в заявке делается отметка о выполнении задания за дписями исполнителей.

В случае производственной необходимости сохранения персональных документов рофайла пользователя) на АРМ работника после прекращения срока действия его полномочий ециалист отдела кадров (для работников не входящих в штат Поликлиники – руководитель рирующего соответствующие договорные отношения) должен своевременно (не позднее, чем 3 суток до момента прекращения срока действия полномочий пользователя) подать заявку на окирование учетной записи пользователя с указанием срока хранения указанной информации. ивка должна подаваться даже в случае применения механизмов автоматической блокировки етных записей уволенных сотрудников.

Такая заявка должна быть предварительно согласована с администратором формационной безопасности, и после выполнения действий по блокированию учетной записи редается лицу ответственному за информационную безопасность для исполнения

7.1.6. Порядок хранения исполненных заявок

Исполненные заявки передается в отдел информационных технологий, и хранятся в архиве ечение 5 лет с момента окончания предоставления доступа к информационному ресурсу ел информационных технологий для исполнения требования по сохранению данных.

Копии исполненных заявок хранятся у администратора информационной безопасности. и могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий в ИС Поликлиники;
- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам системы при разборе конфликтных ситуаций;
- для проверки администратором информационной безопасности правильности настройки средств разграничения доступа к ресурсам системы.

В случае невозможности исполнения инициатору заявки направляется мотивированный аз с приложением Заявки.

2. Политика учетных записей

2.1. Назначение

Настоящая политика определяет основные правила присвоения учетных записей ьзователям информационных активов Поликлиники.

2.2. Положение политики

Регистрационные учетные записи подразделяются на:

- пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов Поликлиники;
- системные – используемые для нужд операционной системы;
- служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов Поликлиники назначается уникальная зовательская регистрационная учетная запись. Допускается привязка более одной зовательской учетной записи к одному и тому же пользователю (например, имеющих ичный уровень полномочий).

В общем случае запрещено создавать и использовать общую пользовательскую учетную ись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей матизируемого бизнес-процесса или организации труда (например, посменное дежурство), льзование общей учетной записи должно сопровождаться отметкой в журнале учета ченного времени, которая должна однозначно идентифицировать текущего владельца ой записи в каждый момент времени. Одновременное использование одной общей льзовательской учетной записи разными пользователями запрещено.

Системные регистрационные учетные записи формируются операционной системой и жны использоваться только в случаях, предписанных документацией на операционную стему.

Служебные регистрационные учетные записи используются только для запуска сервисов приложений.

Использование системных или служебных учетных записей для регистрации льзователей в системе категорически запрещено.

3. Политика использования паролей

3.1. Назначение

Настоящая политика определяет основные правила обращения с паролями, ользуемыми для доступа к информационным активам Поликлиники.

3.2. Положения политики

Идентификация/аутентификация пользователей осуществляется согласно с требованиями аментирующих документов Российской Федерации посредством использования нтификаторов и/или паролей.

Организационное и техническое обеспечение процессов генерации, использования, смены прекращения действия паролей во всех подсистемах АС Поликлиники и контроль за ствиями исполнителей и обслуживающего персонала системы при работе с паролями агается на администратора информационной безопасности.

Доступ к информационным активам Поликлиники должен производиться с ользованием персональных учетных записей и периодически сменяемых буквенно-ровых паролей, удовлетворяющих следующим требованиям:

- пароль содержит не менее шести символов, включая буквы обоих регистров и цифры;
- не является словом, присутствующим в словарях, или профессиональным термином, в т. ч. набранным в другой раскладке клавиатуры;
- не основывается на семейной, служебной и другой легко доступной информации (фамилии, имена, даты рождения, клички животных, автомобильные и телефонные номера, названия организаций, адреса сайтов и т. п.);
- не содержит легко угадываемые последовательности символов (456789, ooobbb, qwerty, a1s2d3 и т. п.).
- одним из способов создания безопасных, но легко запоминающихся паролей является кодирование стихотворной строки или осмысленного утверждения. Так, пароль, созданный на основе фразы: "Вот один пример надежного и запоминающегося пароля", может быть таким: "HitlGE&BS".

Временный пароль, создаваемый администратором при заведении учетной записи или е забытого пароля, должен быть уникальным, передаваться способом, исключающим уп к нему других лиц, и быть сменен пользователем при первом обращении к активу. ли, предустановленные производителем, должны сменяться до начала эксплуатации ва.

В Поликлинике может применяться резервирование некоторых паролей, таких, как пароли нистраторов информационных систем, пароли ответственных должностных лиц, пароли льных пользователей, выполняющих важные функции, пароли обеспечивающие работу льных сетевых сервисов.

Для резервирования пароля выполняются следующие действия:

- пароль записывается на лист бумаги и заверяется личной подписью;
- лист с записью пароля вкладывается владельцем в конверт. Конверт не должен допускать просмотра записи пароля на просвет. Если конверт недостаточно плотный, в него может быть вложен лист темной бумаги. Конверт заклеивается, при необходимости (для особо важных паролей) - опечатывается;
- на конверте владелец пароля указывает свою должность, фамилию и инициалы, наименование информационного средства, которое защищается этим паролем, текущие дату и время, при необходимости – другие данные, и заверяет запись личной подписью;
- конверт передается на хранение руководителю подразделения или лицу, им для этого назначенного и учитывается в специальном разделе Журнала учета паролей. Учетный номер (сквозной по Журналу) проставляется ответственным за хранение на конверте.

Конверты с паролями хранятся в сейфе. Ответственный за хранение не реже чем один раз в проверяет их наличие по журналу учета.

При замене пароля конверт передается владельцу пароля, который уничтожает лист с ным паролем, о чем делается запись в Журнале учета паролей. Новый резервный пароль тавливает к хранению так, как указано выше. Новый конверт учитывается в Журнале учета ей отдельной позицией.

Вскрытие конверта с паролем производится по решению главного врача в случае одимости использования прав доступа его владельца в отсутствие самого владельца. Для тия конверта назначается комиссия не менее чем из трех сотрудников. О вскрытии рта комиссией составляется акт, утверждаемый руководителем подразделения, который по ании работы комиссии хранится в деле подразделения.

При появлении владельца пароля после факта вскрытия конверта пароль заменяется на и вновь сохраняется его копия, как описано выше.

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже раза в три месяца.

Внеплановая смена личного пароля или удаление учетной записи пользователя тизированной системы проводится в случае прекращения его полномочий (увольнение, од на другую работу внутри территориального органа организации и т.п.) производится истратором информационной безопасности немедленно после окончания последнего работы данного пользователя с системой. Ответственность за своевременное тавление сведений о перемещении сотрудников несет специалист по кадрам.

Внеплановая полная смена паролей всех пользователей должна производиться в случае щения полномочий (увольнение, переход на другую работу внутри территориального организации и другие обстоятельства) администратора информационной безопасности истраторов средств защиты и других сотрудников), которым по роду работы были тавлены полномочия по управлению парольной защитой подсистем АС.

случае компрометации личного пароля пользователя автоматизированной системы ится внеплановая смена пароля в зависимости от полномочий владельца ометированного пароля.

Повседневный контроль за действиями исполнителей и обслуживающего персонала ы при работе с паролями, соблюдением порядка их смены, хранения и использования ается на ответственных за информационную безопасность в подразделениях одителей подразделений), периодический контроль – возлагается на сотрудников отдела мационных технологий и администратора информационной безопасности.

ЗАПРЕЩАЕТСЯ:

- сообщать свой персональный пароль другим лицам или записывать его на материальных носителях, доступных для других лиц (кроме предусмотренных случаев сохранения паролей ключевых учетных записей владельцем информационного актива);
- сохранять пароль в программно-технических средствах в открытом виде или использовать средства его автоматического ввода;

- использовать легко угадываемый алгоритм смены пароля (например, F%1hTR8 -* F%2hTR8 -> F%3hTR8, или F%1hTR8 -* Fl%hTR8 -* F1h%TR8 и др.);
- использовать учетные записи других лиц;
- использовать вне Поликлиники пароли, совпадающие с паролями доступа к его информационно-технологическим активам;
- использовать в качестве паролей примеры, приведенные в Политике.

В зависимости от критичности информационно-технологического актива, его владельцем ут быть установлены более высокие требования к сложности пароля и периодичности ны.

Процессы создания, изменения, использования, блокирования, удаления учетных записей, также смены паролей должны быть регламентированы, протоколироваться и тролироваться.

.4. Политика реализации антивирусной защиты

.4.1. Назначение

Настоящая Политика определяет основные правила для реализации антивирусной защиты оликлиники.

.4.2. Положения политики

Средства антивирусной защиты выполняют функции по ограничению распространения усной атаки и ее локализации.

В состав средств антивирусной защиты входят следующие компоненты:

- средства управления, включающие в себя управляющую консоль, серверные компоненты системы антивирусной защиты, средства протоколирования и генерации отчетов;
- средства антивирусной защиты серверов ЛВС;
- средства антивирусной защиты рабочих станций;
- средства антивирусной защиты почтовой системы (внутренних почтовых серверов и SMTP-шлюзов на внешнем периметре сети);
- антивирусный шлюз, осуществляющий антивирусный контроль HTTP и FTP трафика.

В качестве средств антивирусной защиты в Поликлиники применяется NOD 32® – для ивирусной защиты АРМ внутренних пользователей и серверов.

Настоящая Политика предназначена для пользователей, хранящих и обрабатывающих юрмацию в ИС Поликлиники.

В целях обеспечения антивирусной защиты в АС производится антивирусный контроль. етственность за поддержание установленного в настоящей Политики порядка проведения ивирусного контроля возлагается на отдел информационных технологий и администратора юрмационной безопасности.

Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при езапуске) в автоматическом режиме должно выполняться обновление антивирусных баз и водиться антивирусный контроль всех дисков и файлов персонального компьютера.

Администратор информационной безопасности осуществляет контроль обновления ивирусных пакетов, контроль их работоспособности, проводит периодическое тестирование о установленного программного обеспечения на предмет отсутствия компьютерных усов. Периодические проверки электронных архивов должны проводиться не реже одного в неделю.

Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера жен выполняться:

- непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка: на серверах и персональных компьютерах учреждения. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего.
- при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

Пользователи АС при работе с отчуждаемыми носителями информации обязаны перед ом работы осуществить их проверку на предмет отсутствия компьютерных вирусов. с для запуска антивирусной программы должен быть вынесен в окно "Рабочий стол" ционной системы Windows XP.

В случае обнаружения при проведении антивирусной проверки зараженных ютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность администратора информационной безопасности или программиста о факте обнаружения зараженных вирусом файлов;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения на отчуждаемых носителях информации нового вируса, не поддающегося лечению, администратор информационной безопасности обязан запретить использование отчуждаемых носителей информации;
- в случае обнаружения на ЖМД не поддающегося лечению вируса, администратор информационной безопасности о запретить работу в АС и в возможно короткие сроки обновить пакет антивирусных программ.

Политика защиты АРМ

1. Назначение

Настоящая Политика определяет основные правила и требования по защите денциальной информации Поликлиники от неавторизованного доступа, утраты или ификации.

2. Положения политики

о время работы с конфиденциальной информацией должен предотвращаться ее просмотр ущенными к ней лицами.

ри любом оставлении рабочего места, рабочая станция должна быть заблокирована, ие машинные носители, содержащие конфиденциальную информацию, заперты в ении, шкафу или ящике стола или в сейфе.

есанкционированное использование печатающих, факсимильных, копировально-тельных аппаратов и сканеров должно предотвращаться путем их размещения в ениях с ограниченным доступом, использования паролей или иных доступных змов разграничения доступа.

отрудники получают доступ к ресурсам вычислительной сети после ознакомления с нтами, утвержденными стандартами учреждения, (согласно занимаемой должности).

оступ к компонентам операционной системы и командам системного администрирования очих станциях пользователей ограничен. Право на доступ к подобным компонентам тавлено только специалистам отдела информационных технологий. Конечным

пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к корпоративной информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя лицу ответственному ха информационную безопасность, а все обращения должны регистрироваться.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

Программное обеспечение должно устанавливаться со специальных сетевых ресурсов или съемных носителей, маркированных отделом информационных технологий, и в соответствии с лицензионным соглашением с его правообладателем.

Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию - регламентированы.

АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими работниками Поликлиники. Запрещается использование указанных АРМ другими пользователями без согласования с лицом ответственным за ИБ. При передаче указанного АРМ другому пользователю, должна производится гарантированная очистка диска (форматирование).

Лицо ответственное за информационную безопасность вправе отказать в устранении проблемы, вызванной наличием на рабочем месте программного обеспечения или оборудования, установленного или настроенного пользователем в обход действующей процедуры.

3.8. Порядок сопровождения ИС Поликлиники

Обеспечение информационной безопасности информационных систем на стадиях жизненного цикла ИБ ИС должна обеспечиваться на всех стадиях жизненного цикла (ЖЦ) ИС, автоматизирующих технологические процессы, с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений организации). Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты ИС проводится при участии отдела информационных технологий. Порядок разработки и внедрения ИС должен быть регламентирован и контролироваться.

При разработке ИС необходимо придерживаться требований и методических указаний определенных стандартами, входящими в группу ГОСТ 34.ххх "Стандарты информационной технологии".

Ввод в действие, эксплуатация, снятие с эксплуатации ИС в части вопросов ИБ должны осуществляться при участии отдела информационных технологий.

На стадиях, связанных с разработкой ИС (определение требований заинтересованных ен, анализ требований, архитектурное проектирование, реализация, интеграция и фикация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от з:

- неверной формулировки требований к ИС;
- выбора неадекватной модели ЖЦ ИС, в том числе неадекватного выбора процессов ЖЦ и вовлеченных в них участников;
- принятия неверных проектных решений;
- внесения разработчиком дефектов на уровне архитектурных решений;
- внесения разработчиком недокументированных возможностей в ИС;
- неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к ИС;
- разработки некачественной документации;
- сборки ИС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований;
- неверного конфигурирования ИС;
- приемки ИС, не отвечающей требованиям заказчика;
- внесения недокументированных возможностей в ИС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

Привлекаемые для разработки и (или) производства средств и систем защиты ИС на орной основе специализированные организации должны иметь лицензии на данный вид льности в соответствии с законодательством РФ.

При приобретении готовых ИС и их компонентов разработчиком должна быть ставлена документация, содержащая, в том числе, описание защитных мер, предпринятых ботчиком в отношении угроз информационной безопасности.

Также разработчиком должна быть представлена документация, содержащая описание ных мер, предпринятых разработчиком ИС и их компонентов относительно безопасности ботки, безопасности поставки, эксплуатации, поддержки жизненного цикла, включая ние модели жизненного цикла, оценки уязвимости. Данная документация может быть тавлена в рамках декларации о соответствии или быть результатом оценки соответствия ия, проведенной в рамках соответствующей системы оценки.

В договор (контракт) о поставке ИС и их компонентов рекомендуется включать положения провождению поставляемых изделий на весь срок их службы. В случае невозможности ения в договор (контракт) указанных требований к разработчику должна быть отрена возможность приобретения полного комплекта рабочей конструкторской ентации на изделие, обеспечивающее возможность сопровождения ИС и их компонентов частия разработчика. Если оба указанных варианта неприемлемы, например, вследствие ой стоимости, руководство Поликлиники должно обеспечить анализ влияния угрозы можности сопровождения ИС и их компонентов на обеспечение непрерывности водственного процесса.

На стадии эксплуатации должна быть обеспечена защита от следующих угроз:

- умышленное несанкционированное раскрытие, модификация или уничтожение информации;
- неумышленная модификация или уничтожение информации;
- недоставка или ошибочная доставка информации;
- отказ в обслуживании или ухудшение обслуживания.

Кроме этого, актуальной является угроза отказа от авторства сообщения. На стадии ождения должна быть обеспечена защита от угроз:

- внесения изменений в ИС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей;

– невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния ИС.

На стадии снятия с эксплуатации должно быть обеспечено удаление информации, анкционированное использование которой может нанести ущерб Поликлиники, и формации, используемой средствами обеспечения ИБ, из постоянной памяти ИС или с ших носителей.

Требования ИБ должны включаться во все договора и контракты на проведение работ или зание услуг на всех стадиях ЖЦ ИС.

3.1. Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений Политик информационной безопасности понимается ведение регламентных работ по защите информации, предупреждение возможных рушений информационной безопасности в Поликлинике и проведение разъяснительной боты по информационной безопасности среди пользователей Поликлиники.

Проведение в ИС Поликлиники регламентных работ по защите информации предполагает полнение процедур контрольного тестирования (проверки) функций СЗИ, что гарантирует ее ботоспособность с точностью до периода тестирования. Контрольное тестирование функций И может быть частичным или полным и должно проводиться с установленной в ИС диклиники степенью периодичности.

Задача предупреждения в ИС Поликлиники возможных нарушений информационной юпасности решается по мере наступления следующих событий:

- включение в состав ИС Поликлиники новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Поликлиники;
- изменение конфигурации программных и технических средств ИС Поликлиники (изменение конфигурации программного обеспечения рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Поликлиники;
- при появлении сведений о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения технических средств, используемых в ИС Поликлиники.

Сотрудник ответственный за ИБ (возможно, при помощи сторонней организации ециализирующейся в области информационной безопасности) собирает и анализирует формацию о выявленных уязвимых местах в составе операционных систем и/или ограммного обеспечения относительно ИС Поликлиники. Источниками подобного рода ведений могут служить официальные издания и публикации различных компаний, щественных объединений и других организаций, специализирующихся в области защиты формации.

Сотрудник ответственный за ИБ (возможно, при помощи сторонней организации, ециализирующейся в области информационной безопасности) организовывает риодическую проверку СЗИ ИС Поликлиники путем моделирования возможных попыток уществления НСД к защищаемым информационным ресурсам.

Для решения задач контроля защищенности ИС используются инструментальные средства я тестирования реализованных в составе СЗИ ИС Поликлиники средств и функций защиты. результатам профилактических работ, проводимых в ИС Поликлиники, необходимо сделать ответствующие записи в специальном журнале.

Плановая разъяснительная работа по правилам настоящих Политик, а также инструктаж ботников Поликлиники по соблюдению требований нормативных и регламентных кументов по информационной безопасности, принятых в Поликлинике, проводится министратором информационной безопасности ежеквартально.

Внеплановая разъяснительная работа по правилам настоящих Политик, а также структаж работников Поликлиники по соблюдению требований нормативных и регламентных кументов по информационной безопасности, принятых в Поликлинике, проводится при

есмотре настоящих Политик, при возникновении инцидента нарушения правил настоящих итик.

Прием на работу новых сотрудников должен сопровождаться ознакомлением их с вилами и требованиями настоящих Политик.

2. Ликвидация последствий нарушения политик информационной безопасности

Администратор информационной безопасности, используя данные, полученные в льтате применения инструментальных средств контроля (мониторинга) безопасности ормации ИС Поликлиники, должны своевременно обнаруживать нарушения ормационной безопасности, факты осуществления НСД к защищаемым информационным рсам и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения ормационной безопасности или осуществления НСД к защищаемым информационным рсам ИС Поликлиники рекомендуется уведомить администратора информационной пасности и отдел информационных технологий, и далее следовать их указаниям.

Действия специалистов и пользователей ИС при признаках нарушения Политик ормационной безопасности регламентируются следующими внутренними документами:

- Инструкцией пользователя автоматизированной системы;
- Стандартом информационной безопасности Поликлиники;
- Положением об Отделе информационных технологий.

После устранения инцидента необходимо составить акт о факте нарушения и принятых их по восстановлению работоспособности ИС Поликлиники, а также зарегистрировать факт шения в журнале учета нарушений, ликвидации их причин и последствий.

3. Ответственность нарушителей ПБ

Ответственность за выполнение правил Политик безопасности несет каждый работник иклиники в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования тики безопасности Поликлиники, могут быть подвергнуты дисциплинарным взысканиям, учая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за ой действительный ущерб, причиненный Поликлиники в результате нарушения ими правил тики ИБ (Ст. 238 Трудового кодекса РФ).

За умышленное причинение ущерба, а также за разглашение сведений, составляющих няемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных ральными законами, сотрудники Поликлиники несут материальную ответственность в ом размере причиненного ущерба (Ст. 243 Трудового кодекса РФ).

За неправомерный доступ к компьютерной информации, создание, использование или остранение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, ствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки рмации), уничтожение, блокирование или модификация защищаемой информации, дники Поликлиники несут ответственность в соответствии со статьями 272, 273 и 274 овного кодекса Российской Федерации.

4. Регулирующие законодательные нормативные документы

Ірн организации и обеспечении работ по информационной безопасности работники клиники должны руководствоваться следующими законодательными нормативными ентами:

Основополагающие нормативные документы

К основополагающим нормативным документам относятся:

- Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.);
- Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов (разработана во исполнение Указа Президента Российской Федерации от 1 июля 1994 г. № 1390 "О совершенствовании информационно-телекоммуникационного обеспечения органов государственной власти и порядке их взаимодействия при реализации государственной политики в сфере информатизации");
- Концепция национальной безопасности Российской Федерации (утверждена Указом Президента РФ от 17 декабря 1997 г. № 1300, в редакции Указа Президента РФ от 10 января 2000 г. № 24);
- Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ от 9 сентября 2000 г. № Пр-1895).

Законы Российской Федерации

- Закон Российской Федерации от 5 марта 1992 г. № 2446-I "О безопасности" (с изменениями от 25 декабря 1992 г., 24 декабря 1993 г., 25 июля 2002 г., 7 марта 2005 г., 25 июля 2006 г., 2 марта 2007 г.);
- Гражданский кодекс Российской Федерации часть первая от 30 ноября 1994 г. № 51-ФЗ, часть вторая от 26 января 1996 г. № 14-ФЗ, часть третья от 26 ноября 2001 г. № 146-ФЗ и часть четвертая от 18 декабря 2006 г. № 230-ФЗ (с изменениями от 26 января, 20 февраля, 12 августа 1996 г., 24 октября 1997 г., 8 июля, 17 декабря 1999 г., 16 апреля, 15 мая, 26 ноября 2001 г., 21 марта, 14, 26 ноября 2002 г., 10 января, 26 марта, 11 ноября, 23 декабря 2003 г., 29 июня, 29 июля, 2, 29, 30 декабря 2004 г., 21 марта, 9 мая, 2, 18, 21 июля 2005 г., 3, 10 января, 2 февраля, 3, 30 июня, 27 июля, 3 ноября, 4, 18, 29, 30 декабря 2006 г., 26 января, 5 февраля, 20 апреля, 26 июня, 19, 24 июля, 2, 25 октября, 4, 29 ноября, 1, 6 декабря 2007 г.);
- Закон Российской Федерации от 27 ноября 1992 г. № 4015-I "Об организации страхового дела в Российской Федерации" (с изменениями от 31 декабря 1997 г., 20 ноября 1999 г., 21 марта, 25 апреля 2002 г., 8, 10 декабря 2003 г., 21 июня, 20 июля 2004 г., 7 марта, 18, 21 июля 2005 г., 17 мая, 8, 29 ноября 2007 г.);
- Федеральный закон от 21 декабря 1994 г. № 69-ФЗ "О пожарной безопасности" (с изменениями от 22 августа 1995 г., 18 апреля 1996 г., 24 января 1998 г., 7 ноября, 27 декабря 2000 г., 6 августа, 30 декабря 2001 г., 25 июля 2002 г., 10 января 2003 г., 10 мая, 29 июня, 22 августа, 29 декабря 2004 г., 1 апреля, 9 мая 2005 г., 2 февраля, 25 октября, 4, 18 декабря 2006 г., 26 апреля, 18 октября 2007 г.);
- Федеральный закон от 12 августа 1995 г. № 144-ФЗ "Об оперативно-розыскной деятельности" (с изменениями от 18 июля 1997 г., 21 июля 1998 г., 5 января, 30 декабря 1999 г., 20 марта 2001 г., 10 января, 30 июня 2003 г., 29 июня, 22 августа 2004 г., 2 декабря 2005 г., 24 июля 2007 г.);
- Федеральный закон от 10 января 2002 г. № 1-ФЗ "Об электронной цифровой подписи" (с изменениями от 8 ноября 2007 г.);
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных";

- Закон Российской Федерации от 21 июля 1993 г. № 5485-1 "О государственной тайне" (с изменениями от 6 октября 1997 г., 30 июня, 11 ноября 2003 г., 29 июня, 22 августа 2004 г., 1 декабря 2007 г.);
- Федеральный закон от 7 июля 2003 г. № 126-ФЗ "О связи" (с изменениями от 23 декабря 2003 г., 22 августа, 2 ноября 2004 г., 9 мая 2005 г., 2 февраля, 3 марта, 26 июля, 29 декабря 2006 г., 9 февраля, 24 июля 2007 г.);
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федеральный закон от 3 апреля 1995 г. № 40-ФЗ "О федеральной службе безопасности" (с изменениями от 30 декабря 1999 г., 7 ноября 2000 г., 30 декабря 2001 г., 7 мая, 25 июля 2002 г., 10 января, 30 июня 2003 г., 22 августа 2004 г., 7 марта 2005 г., 15 апреля, 27 июля 2006 г., 5, 24 июля, 4 декабря 2007 г.);
- Федеральный закон от 9 января 1996 г. № 2-ФЗ "О внесении изменений и дополнений в Закон Российской Федерации "О защите прав потребителей" и Кодекс РСФСР об административных правонарушениях" (с изменениями от 30 декабря 2001 г., 25 октября 2007 г.);
- Федеральный закон от 9 января 1996 г. № 3-ФЗ "О радиационной безопасности населения" (с изменениями от 22 августа 2004 г.);
- Федеральный закон от 10 января 1996 г. № 5-ФЗ "О внешней разведке" (с изменениями от 7 ноября 2000 г., 30 июня 2003 г., 22 августа 2004 г., 14 февраля 2007 г.);
- Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ (с изменениями от 27 мая, 25 июня 1998 г., 9 февраля, 15, 18 марта, 9 июля 1999 г., 9, 20 марта, 19 июня, 7 августа, 17 ноября, 29 декабря 2001 г., 4, 14 марта, 7 мая, 25 июня, 24, 25 июля, 31 октября 2002 г., 11 марта, 8 апреля, 4, 7 июля, 8 декабря 2003 г., 21, 26 июля, 28 декабря 2004 г., 21 июля, 19 декабря 2005 г., 5 января, 27 июля, 4, 30 декабря 2006 г., 9 апреля, 10 мая, 24 июля, 4 ноября, 1, 6 декабря 2007 г.);
- Федеральный закон от 13 декабря 1996 г. № 150-ФЗ "Об оружии" (с изменениями от 21, 31 июля, 17 декабря 1998 г., 19 ноября 1999 г., 10 апреля 2000 г., 26 июля, 8 августа, 27 ноября 2001 г., 25 июня, 25 июля 2002 г., 10 января, 30 июня, 8 декабря 2003 г., 26 апреля, 29 июня 2004 г., 18 июля, 29 декабря 2006 г., 24 июля 2007 г.);
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ "О техническом регулировании" (с изменениями от 9 мая 2005 г., 1 мая, 1 декабря 2007 г.);
- Федеральный закон от 8 августа 2001 г. № 128-ФЗ "О лицензировании отдельных видов деятельности" (с изменениями от 13, 21 марта, 9 декабря 2002 г., 10 января, 27 февраля, 11, 26 марта, 23 декабря 2003 г., 2 ноября 2004 г., 21 марта, 2 июля, 31 декабря 2005 г., 27 июля, 4, 29 декабря 2006 г., 5 февраля, 19 июля, 4, 8 ноября, 1, 6 декабря 2007 г.).

Указы и распоряжения президента Российской Федерации

- Указ Президента Российской Федерации от 14 января 1992 г. № 20 "О защите государственных секретов Российской Федерации";
- Указ Президента Российской Федерации от 7 октября 1993 г. № 1607 "О государственной политике в области охраны авторского права и смежных прав";
- Указ Президента Российской Федерации от 31 декабря 1993 г. № 2334 "О дополнительных гарантиях прав граждан на информацию" (с изменениями от 17 января 1997 г., 1 сентября 2000 г.);
- Указ Президента Российской Федерации от 20 января 1994 г. № 170 "Об основах государственной политики в сфере информатизации" (с изменениями от 26 июля 1995 г., 17 января, 9 июля 1997 г.);
- Указ Президента Российской Федерации от 3 апреля 1995 г. № 334 "О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации" (с изменениями от 25 июля 2000 г.);

- Указ Президента Российской Федерации от 3 июля 1995 г. № 662 "О мерах по формированию общероссийской телекоммуникационной системы и обеспечению прав собственников при хранении ценных бумаг и расчетах на фондовом рынке Российской Федерации" (с изменениями от 16 августа 1995 г., 4 января 1996 г., 28 мая 1997 г., 29 ноября 2004 г.);
- Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 "Об утверждении перечня сведений, отнесенных к государственной тайне" (с изменениями от 24 января 1998 г., 6 июня, 10 сентября 2001 г., 29 мая 2002 г., 3 марта 2005 г., 11 февраля 2006 г., 24 декабря 2007 г.);
- Указ Президента Российской Федерации от 9 января 1996 г. № 21 "О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации" (с изменениями от 30 декабря 2000 г.);
- Указ Президента Российской Федерации от 17 декабря 1997 г. № 1300 "Об утверждении Концепции национальной безопасности Российской Федерации" (с изменениями от 10 января 2000 г.);
- Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" (с изменениями от 22 марта, 20 июля 2005 г., 30 ноября 2006 г.);
- Указ Президента Российской Федерации от 6 октября 2004 г. № 1286 "Вопросы Межведомственной комиссии по защите государственной тайны";
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 "Об утверждении перечня сведений конфиденциального характера" (с изменениями от 23 сентября 2005 г.);
- Распоряжение Президента Российской Федерации от 16 апреля 2005 г. № 151-рп "О перечне должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне" (с изменениями от 12 октября 2007 г.).

Постановления и распоряжения правительства Российской Федерации

- Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти";
- Постановление Правительства Российской Федерации от 26 января 2006 г. № 45 "Об организации лицензирования отдельных видов деятельности" (с изменениями от 5 мая, 3 сентября, 2 октября 2007 г.);
- Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны" (с изменениями от 23 апреля 1996 г., 30 апреля 1997 г., 29 июля 1998 г., 3 октября 2002 г., 17 декабря 2004 г., 26 января 2007 г.);
- Постановление Правительства Российской Федерации от 29 декабря 2007 г. № 957 "Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами";
- Постановление Правительства РФ от 31 августа 2006 г. № 532 "О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации";

- Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 "О сертификации средств защиты информации" (с изменениями от 23 апреля 1996 г., 29 марта 1999 г., 17 декабря 2004 г.);
- Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870 "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности" (с изменениями от 15 января 2008 г.);
- Постановление Правительства Российской Федерации от 15 августа 2006 г. № 504 "О лицензировании деятельности по технической защите конфиденциальной информации";
- Постановление Правительства Российской Федерации от 1 июля 1996 г. № 770 "Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности" (с изменениями от 15 июля 2002 г.);
- Постановление Правительства Российской Федерации от 2 августа 1997 г. № 973 "Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам";

5. Нормативные и руководящие документы Федеральных служб РФ

- Решение Гостехкомиссии России от 21 октября 1997 г. № 61 "О защите информации при вхождении России в международную информационную систему "Интернет";
- Приказ Федеральной службы по техническому и экспортному контролю от 28 августа 2007 г. № 181 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по технической защите конфиденциальной информации";
- Приказ ФСБ Российской Федерации от 9 февраля 2005 г. № 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)";
- Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР) (утверждено решением Гостехкомиссии России от 23 мая 1997 г. № 55-с);
- Постановление Госстандарта Российской Федерации от 21 сентября 1994 г. № 15 "Об утверждении "Порядка проведения сертификации продукции в Российской Федерации" (с изменениями от 25 июля 1996 г., 11 июля 2002 г.);
- Постановление Госстандарта Российской Федерации от 10 мая 2000 г. № 26 "Об утверждении Правил по проведению сертификации в Российской Федерации" (с изменениями от 5 июля 2002 г.);
- Положение о сертификации средств защиты информации по требованиям безопасности информации (утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. № 199);
- Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.);
- Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации (утверждено

Председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.);

- Типовое положение об испытательной лаборатории (утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 25 ноября 1994 г.);
- Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации (утверждено приказом председателя
- Государственной технической комиссии при Президенте Российской Федерации т 5 января 1996 г. № 3);
- Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);
- 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 (утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);
- Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);
- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);
- Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения (утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.);
- Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.);
- Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.);
- Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114);
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (введен в действие Приказом Гостехкомиссии России от 19.06.02 г. № 187);
- Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации, Гостехкомиссия России, Москва, 2002;
- Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт

наводок на вспомогательные технические средства и системы и их коммуникации, Гостехкомиссия России, Москва, 2002;

- Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам, Гостехкомиссия России, Москва, 2002;
- Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах, Гостехкомиссия России, Москва, 2002;
- Нормативно-методический документ. Специальные требования и рекомендации по технической защите конфиденциальной информации (утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282);
- Приказ Минэнерго Российской Федерации от 13 января 2003 г. № 6 "Об утверждении Правил технической эксплуатации электроустановок потребителей";
- Приказ Федерального агентства по техническому регулированию и метрологии от 22 июня 2006 г. № 119-ст "О введении в действие межгосударственных стандартов";
- Руководящий документ РД 50-082-89 "Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Основные положения", 1989 г.;
- Руководящий документ РД 50-34.698-90 "Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Требования к содержанию документов", 1990 г.;
- Руководящий документ РД 50-680-88 "Методические указания. Автоматизированные системы. Основные положения", 1988 г.;
- Рекомендация Р 50-34.119-90 "Рекомендации. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Архитектура локальных вычислительных сетей в системах промышленной автоматизации. Общие положения", 1990 г.;
- Рекомендация Р 50.4.002-2000 "Рекомендации по аккредитации. Инспекционный контроль за деятельностью в системе сертификации", 2000 г.;
- Рекомендация МИ 2377-98 "Рекомендация. Государственная система обеспечения единства измерений. Разработка и аттестация методик выполнения измерений", 1998 г.;
- Методические указания МИ 1317-86 "Методические указания. Государственная система обеспечения единства измерений. Результаты и характеристики погрешности измерений. Формы представления. Способы использования при испытаниях образцов продукции и контроля их параметров", 1986 г.;
- Строительные нормы и правила СНиП 23-03-2003 "Защита от шума" (введены в ействие постановлением Госстроя РФ от 30 июня 2003 г. № 136);
- Письмо Министерства промышленности и энергетики Российской Федерации и Министерства регионального развития Российской Федерации от 29 ноября 2006 г. № АР-6893/08, 12325-ЮТ/08;
- Постановление Главного государственного санитарного врача Российской Федерации от 3 июня 2003 г. № 118 "О введении в действие санитарно- эпидемиологических правил и нормативов СанПиН 2.2.2/2.4.1340-03" (с изменениями от 25 апреля 2007 г.);
- Нормы пожарной безопасности НПБ 88-2001 "Установки пожаротушения и сигнализации. Нормы и правила проектирования" (утверждены приказом ГУГПС МВД РФ от 4 июня 2001 г. N 31, с изменениями от 31 декабря 2002 г.);
- Строительные нормы и правила СНиП 2.01.15-90 "Инженерная защита территорий, зданий и сооружений от опасных геологических процессов. Основные положения проектирования" (утверждены постановлением Госстроя СССР от 29 декабря 1990 г. № 118);
- Строительные нормы и правила СНиП 41-01-2003 "Отопление, вентиляция и кондиционирование" (приняты постановлением Госстроя РФ от 26 июня 2003 г. № 115);

- Строительные нормы и правила СНиП 21-01-97 "Пожарная безопасность зданий и сооружений" (утверждены постановлением Минстроя РФ от 13 февраля 1997 г. № 18-7, с изменениями от 3 июня 1999 г., 19 июля 2002 г.).

6. Государственные стандарты

- ГОСТ 2.051-2006 "Единая система конструкторской документации. Электронные документы. Общие положения" (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 июня 2006 г. № 119-ст);
- ГОСТ 2.101-68 "Единая система конструкторской документации. Виды изделий" (утвержден Госстандартом СССР в декабре 1967 г.);
- ГОСТ 2.102-68 "Единая система конструкторской документации. Виды и комплектность конструкторских документов" (утвержден постановлением Госстандарта СССР от 28 июня 1968 г. № 1029, изменениями от 22 июня 2006 г.);
- ГОСТ 2.103-68 "Единая система конструкторской документации. Стадии разработки" (введен в действие Госстандартом СССР в декабре 1967 г., с изменениями от 22 июня 2006 г.);
- ГОСТ 2.601-2006 "Единая система конструкторской документации. Эксплуатационные документы" (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 июня 2006 г. № 118-ст);
- ГОСТ 2.111-68 "Единая система конструкторской документации. Нормоконтроль" (утвержден Госстандартом СССР в декабре 1967 г., с изменениями от 22 июня 2006 г.);
- ГОСТ 18321-73 "Статистический контроль качества. Методы случайного отбора выборок штучной продукции" (введен в действие постановлением Государственного комитета стандартов Совета Министров СССР от 9 января 1973 г. № 33);
- ГОСТ 2.109-73 "Единая система конструкторской документации. Основные требования к чертежам" (утвержден постановлением Госстандарта СССР от 27 июля 1973 г. № 1843, с изменениями от 22 июня 2006 г.);
- ГОСТ 2.118-73 "Единая система конструкторской документации. Техническое предложение" (введен постановлением Госстандарта СССР от 28 февраля 1973 г. № 500, с изменениями от 22 июня 2006 г.);
- ГОСТ 2.119-73 "Единая система конструкторской документации. Эскизный проект" (введен в действие постановлением Госстандарта СССР от 28 февраля 1973 г. № 501, с изменениями от 22 июня 2006 г.);
- ГОСТ 2.120-73 "Единая система конструкторской документации. Технический проект" (введен в действие постановлением Госстандарта СССР от 28 февраля 1973 г. № 502, с изменениями от 22 июня 2006 г.);
- ГОСТ 19.001-77 "Единая система программной документации. Общие положения" (введен в действие постановлением Госстандарта СССР от 20 мая 1977 г. № 1268);
- ГОСТ 19.101-77 "Единая система программной документации. Виды программ и программных документов" (введен в действие постановлением Госстандарта СССР от 20 мая 1977 г. № 1268, с изменениями от июня 1981 г.);
- ГОСТ 19.102-77 "Единая система программной документации. Стадии разработки" (введен в действие постановлением Госстандарта СССР от 20 мая 1977 г. № 1268);
- ГОСТ 19.103-77 "Единая система программной документации. Обозначения программ и программных документов" (введен в действие постановлением Госстандарта СССР от 20 мая 1977 г. № 1268);
- ГОСТ Р 50779.10-2000 (ИСО 3534.1-93) "Статистические методы. Вероятность и основы статистики. Термины и определения" (введен в действие постановлением Госстандарта России от 29 декабря 2000 N 429-ст);
- ГОСТ Р 50779.11-2000 (ИСО 3534.2-93) "Статистические методы. Статистическое управление качеством. Термины и определения" (введен в действие постановлением Госстандарта России от 29 декабря 2000 N 429-ст);

- ГОСТ 19.104-78 "Единая система программной документации. Основные надписи" (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3351, с изменениями от сентября 1981 г.);
- ГОСТ 19.105-78 "Единая система программной документации. Общие требования к программным документам" (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от сентября 1981 г.);
- ГОСТ 19.106-78 "Единая система программной документации. Требования к программным документам, выполненным печатным способом" (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от сентября 1981 г.);
- ГОСТ 19.201-78 (СТ СЭВ 1627-79) "Единая система программной документации. Техническое задание. Требования к содержанию и оформлению" (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3351, с изменениями от июля 1981 г.);
- ГОСТ 19.202-78 (СТ СЭВ 2090-80) "Единая система программной документации. Спецификация. Требования к содержанию и оформлению" (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3351, с изменениями от сентября 1981 г.);
- ГОСТ 19.401-78 "Единая система программной документации. Текст программы. Требования к содержанию и оформлению" (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от июля 1982 г.);
- ГОСТ 19.402-78 "Единая система программной документации. Описание программы" (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от сентября 1981 г.);
- ГОСТ 19.501-78 "Единая система программной документации. Формуляр. Требования к содержанию и оформлению" (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3351);
- ГОСТ 19.502-78 "Единая система программной документации. Описание применения. Требования к содержанию и оформлению" (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от сентября 1981 г.);
- ГОСТ 19.601-78 "Единая система программной документации. Общие правила дублирования, учета и хранения" (введен в действие постановлением Госстандарта СССР от 22 февраля 1978 г. № 518);
- ГОСТ 19.602-78 "Единая система программной документации. Правила дублирования, учета и хранения программных документов, выполненных печатным способом" (введен в действие постановлением Госстандарта СССР от 22 февраля 1978 г. № 518);
- ГОСТ 19.603-78 "Единая система программной документации. Общие правила внесения изменений" (введен в действие постановлением Госстандарта СССР от 22 февраля 1978 г. № 518, с изменениями от сентября 1981 г.);
- ГОСТ 19.604-78 "Единая система программной документации. Правила внесения изменений в программные документы, выполненные печатным способом" (введен в действие постановлением Госстандарта СССР от 22 февраля 1978 г. № 518, с изменениями от сентября 1981 г.);
- ГОСТ 19.403-79 "Единая система программной документации. Ведомость держателей подлинников" (введен в действие постановлением Госстандарта СССР от 28 июня 1979 г. № 2335);
- ГОСТ 19.404-79 "Единая система программной документации. Пояснительная записка. Требования к содержанию и оформлению" (введен в действие постановлением Госстандарта СССР от 11 декабря 1979 г. № 4753);
- ГОСТ 19.301-79 "Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению" (введен в действие постановлением Госстандарта СССР от 11 декабря 1979 г. № 4753, с изменениями от февраля 1982 г.);

- ГОСТ 19.503-79 "Единая система программной документации. Руководство системного программиста. Требования к содержанию и оформлению" (введен в действие постановлением Госстандарта СССР от 12 января 1979 г. № 74, с изменениями от сентября 1981 г.);
- ГОСТ 19.504-79 "Единая система программной документации. Руководство программиста. Требования к содержанию и оформлению" (введен в действие постановлением Госстандарта СССР от 12 января 1979 г. № 74, с изменениями от сентября 1981 г.);
- ГОСТ 19.505-79 "Единая система программной документации. Руководство оператора. Требования к содержанию и оформлению" (введен в действие постановлением Госстандарта СССР от 12 января 1979 г. № 74, с изменениями от сентября 1981 г.);
- ГОСТ 19.506-79 "Единая система программной документации. Описание языка. Требования к содержанию и оформлению" (введен в действие постановлением Госстандарта СССР от 12 января 1979 г. № 74, с изменениями от сентября 1981 г.);
- ГОСТ 19.507-79 "Единая система программной документации. Ведомость эксплуатационных документов" (введен в действие постановлением Госстандарта СССР от 28 июня 1979 г. № 2335, с изменениями от сентября 1981 г.);
- ГОСТ 19.508-79 "Единая система программной документации. Руководство по техническому обслуживанию. Требования к содержанию и оформлению" (введен в действие постановлением Госстандарта СССР от 11 декабря 1979 г. № 4753);
- ГОСТ 17168-82 (СТ СЭВ 1807-79) "Фильтры электронные октавные и третьоктавные. Общие технические требования и методы испытаний" (введен в действие постановлением Госстандарта СССР от 29 марта 1979 г. № 1294);
- ГОСТ 12.1.003-83 (СТ СЭВ 1930-79) "Система стандартов безопасности труда. Шум. Общие требования безопасности" (утвержден постановлением Госстандарта СССР от 6 июня 1983 г. № 2473, с изменениями от 19 декабря 1988 г.);
- ГОСТ 21552-84 "Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение" (утвержден постановлением Госстандарта СССР от 28 июня 1984 г. № 2206, с изменениями от июня 1987 г., ноября 1988 г., декабря 1990 г.);
- ГОСТ 2.701-84 "Единая система конструкторской документации. Схемы. Виды и типы. Общие требования к выполнению" (утвержден постановлением Госстандарта СССР от 29 августа 1984 г. № 3038);
- ГОСТ 2.124-85 "Единая система конструкторской документации. Порядок применения покупных изделий" (введен в действие постановлением Госстандарта СССР от 13 декабря 1984 г. № 123);
- ГОСТ 12.1.050-86 "Система стандартов безопасности труда. Методы измерения шума на рабочих местах" (введен в действие постановлением Госстандарта СССР от 28 марта 1986 г. № 790, с изменениями от 31 мая 2005 г.);
- ГОСТ 27296-87 (СТ СЭВ 4866-84) "Защита от шума в строительстве. Звукоизоляция ограждающих конструкций. Методы измерения" (введен в действие постановлением Госстроя СССР от 11 сентября 1985 г. № 145);
- ГОСТ 27201-87 "Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования" (утвержден постановлением Госстандарта СССР от 28 января 1987 г. № 124, с изменениями от 24 марта 1989 г., 26 декабря 1990 г.);
- ГОСТ 2.004-88 "Единая система конструкторской документации. Общие требования к выполнению конструкторских и технологических документов на печатающих и графических устройствах вывода ЭВМ" (утвержден постановлением Госстандарта СССР от 28 ноября 1988 г. № 3843);
- ГОСТ 2.125-88 "Единая система конструкторской документации. Правила выполнения эскизных конструкторских документов" (утвержден постановлением Госстандарта СССР от 22 июля 1988 г. № 2714);

- ГОСТ 34.201-89 "Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем" (утвержден постановлением Госстандарта СССР от 24 марта 1989 г. № 664, с изменениями от 29 декабря 1990 г.);
- ГОСТ 34.602-89 "Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы"(утвержден постановлением Госстандарта СССР от 24 марта 1989 г. № 661);
- ГОСТ 28195-89 "Оценка качества программных средств. Общие положения" (утвержден постановлением Госстандарта СССР от 28 июля 1989 г. № 2507);
- ГОСТ 28388-89 "Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения" (утвержден постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 20 декабря 1989 г. № 3903);
- ГОСТ 28806-90 "Качество программных средств. Термины и определения" (утвержден постановлением Госстандарта СССР от 25 декабря 1990 г. № 3278);
- ГОСТ 19.701-90 (ИСО 5807-85) "Единая система программной документации. Схемы алгоритмов, программ, данных и систем. Обозначения условные и правила выполнения" (утвержден постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 26 декабря 1990 г. № 3294);
- ГОСТ 19781-90 "Единая система программной документации. Обеспечение систем обработки информации программное. Термины и определения" (введен в действие постановлением Госстандарта СССР от 27 августа 1990 г. № 2467);
- ГОСТ 34.003-90 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения" (утвержден постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399);
- ГОСТ 2.503-90 "Единая система конструкторской документации. Правила внесения изменений" (утвержден постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 26 апреля 1990 г. № 1031, с изменениями от 22 июня 2006 г.);
- ГОСТ 34.601-90 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы стадии создания" (утвержден постановлением Госстандарта СССР от 29 декабря 1990 г. № 3469);
- ГОСТ 22505-97 "Совместимость технических средств электромагнитная. Радиопомехи индустриальные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний" (утвержден постановлением Госстандарта России от 28 августа 1998 г. № 337);
- ГОСТ 34.603-92 "Информационная технология. Виды испытаний автоматизированных систем" (утвержден постановлением Комитета стандартизации и метрологии СССР от 17 февраля 1992 г. № 161);
- ГОСТ Р ИСО/МЭК ТО 9294-93 "Информационная технология. Руководство по управлению документированием программного обеспечения" (утвержден постановлением Госстандарта России от 20 декабря 1993 г. № 260);
- ГОСТ Р ИСО/МЭК 9126-93 "Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению" (утвержден постановлением Госстандарта России от 28 декабря 1993 г. № 267);
- ГОСТ 2.001-93 "Единая система конструкторской документации. Общие положения" (введен в действие постановлением Госстандарта России от 3 марта 1994 г. № 50, с изменениями от 22 июня 2006 г.);
- ГОСТ 2.123-93 "Единая система конструкторской документации. Комплектность конструкторских документов на печатные платы при автоматизированном проектировании" (введен в действие постановлением Госстандарта России от 2 марта 1994 г. № 44);

- ГОСТ Р ИСО 9127-94 "Системы обработки информации. Документация пользователя и информация на упаковке для потребительских программных пакетов" (принят постановлением Госстандарта России от 10 октября 1994 г. № 242);
- ГОСТ 30373-95/ГОСТ Р 50414-92 "Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний" (принят постановлением Госстандарта России от 15 мая 1996 г. № 308);
- ГОСТ Р 50739-95 "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования" (принят постановлением Госстандарта России от 9 февраля 1995 г. № 49);
- ГОСТ Р 50752-95 "Информационная технология. Защита информации от утечки за счёт побочных электромагнитных излучений при её обработке средствами вычислительной техники. Методы испытаний", Госстандарт России, 1995 г.;
- ГОСТ 2.105-95 "Единая система конструкторской документации. Общие требования к текстовым документам" (введен в действие постановлением Госстандарта России от 8 августа 1995 г. № 426, с изменениями от 22 июня 2006 г.);
- ГОСТ 2.602-95 "Единая система конструкторской документации. Ремонтные документы" (введен в действие постановлением Госстандарта России от 29 февраля 1996 г. № 131, с изменениями от 22 июня 2006 г.);
- ГОСТ 2.106-96 "Единая система конструкторской документации. Текстовые документы" (введен в действие постановлением Госстандарта России от 13 ноября 1996 г. № 620, с изменениями от 22 июня 2006 г.);
- ГОСТ Р 50922-96 "Защита информации. Основные термины и определения" (введен в действие постановлением Госстандарта России от 10 июля 1996 г. № 450);
- ГОСТ Р ИСО 9001-2001 "Системы менеджмента качества. Требования" (утвержден постановлением Госстандарта России от 15 августа 2001 г. № 333-ст, с изменениями от 7 июля 2003 г.);
- ГОСТ 2.780-96 "Единая система конструкторской документации. Обозначения условные графические. Кондиционеры рабочей среды, емкости гидравлические и пневматические" (утвержден постановлением Госстандарта РФ от 7 апреля 1997 г. № 121);
- ГОСТ 2.784-96 "Единая система конструкторской документации. Обозначения условные графические. Элементы трубопроводов" (введен в действие постановлением Госстандарта России от 7 апреля 1997 г. № 124);
- ГОСТ Р 50923-96 "Дисплеи. Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения" (введен в действие постановлением Госстандарта России от 10 июля 1996 г. № 451);
- ГОСТ 22505-97 "Совместимость технических средств электромагнитная. Радиопомехи индустриальные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний" (введен в действие постановлением Госстандарта России от 28 августа 1998 г. № 337);
- ГОСТ Р 51188-98 "Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство" (введен в действие постановлением Госстандарта России от 14 июля 1998 г. № 295);
- ГОСТ Р 51171-98 "Качество служебной информации. Правила предъявления информационных технологий на сертификацию" (введен в действие постановлением Госстандарта России от 12 мая 1998 г. № 184);
- ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения" (введен в действие постановлением Госстандарта России от 12 мая 1999 г. № 160);
- ГОСТ Р ИСО/МЭК 12207-99 "Информационная технология. Процессы жизненного цикла программных средств" (принят и введен в действие постановлением Госстандарта России от 23 декабря 1999 г. № 675-ст);

- ГОСТ Р 51320-99 "Совместимость технических средств электромагнитная. Радиопомехи индустриальные. Методы испытаний технических средств - источников индустриальных радиопомех" (введен в действие постановлением Госстандарта России от 22 декабря 1999 г. № 655-ст);
- ГОСТ Р 50779.72-99 (ИСО 2859-2-85) "Статистические методы. Процедуры выборочного контроля по альтернативному признаку. Часть 2. Планы выборочного контроля отдельных партий на основе предельного качества LQ" (введен в действие постановлением Госстандарта России от 23 декабря 1999 г. № 694-ст);
- ГОСТ Р 51319-99 "Совместимость технических средств электромагнитная. Приборы для измерения индустриальных радиопомех. Технические требования и методы испытаний" (введен в действие постановлением Госстандарта России от 28 декабря 1999 г. № 795-ст);
- ГОСТ Р 51583-2000 "Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения", Госстандарт России, 2000 г.;
- ГОСТ Р 51624-2000 "Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования", Госстандарт России, 2000 г.;
- ГОСТ Р ИСО/МЭК 17025-2006 "Общие требования к компетентности испытательных и калибровочных лабораторий" (введен в действие постановлением Госстандарта России от 27 декабря 2006 г. № 506-ст);
- ГОСТ Р 40.002-2000 "Система сертификации ГОСТ Р. Регистр систем качества. Основные положения" (принят постановлением Госстандарта РФ от 13 апреля
- 2000 г. № 107-ст);
- ГОСТ Р ИСО/МЭК 65-2000 "Общие требования к органам по сертификации продукции" (утвержден постановлением Госстандарта РФ от 7 апреля 2000 г. № 96-ст);
- ГОСТ Р 50628-2000 "Совместимость технических средств электромагнитная. Устойчивость машин электронных вычислительных персональных к электромагнитным помехам. Требования и методы испытаний" (введен в действие постановлением Госстандарта России от 26 декабря 2000 г. № 417-ст);
- ГОСТ Р ИСО 9000-2001 "Системы менеджмента качества. Основные положения и словарь"(принят постановлением Госстандарта России от 15 августа 2001 г. № 332-ст, с изменениями от 7 июля 2003 г.);
- ГОСТ Р ИСО 9004-2001 "Системы менеджмента качества. Рекомендации по улучшению деятельности" (принят постановлением Госстандарта России от 15 августа 2001 г. № 334-ст, с изменениями от 7 июля 2003 г.);
- ГОСТ Р 50948-2001 "Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности" (принят постановлением Госстандарта России от 25 декабря 2001 г. № 576-ст);
- ГОСТ Р 50949-2001 "Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности" (принят постановлением Госстандарта России от 25 декабря 2001 г. № 576-ст);
- 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" (принят постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст);
- ГОСТ Р ИСО/МЭК 15408-2-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности" (принят постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст);
- 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" (принят и введен в действие постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст);

- ГОСТ Р 40.003-2005 "Система сертификации ГОСТ Р. Регистр систем качества. Порядок сертификации систем менеджмента качества на соответствие ГОСТ Р ИСО 9001-2001 (ИСО 9001:2000)" (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 14 ноября 2005 г. № 287-ст);
- ГОСТ Р ИСО/МЭК 17799-2005 "Информационная технология. Практические правила управления информационной безопасностью" (принят постановлением Госстандарта России от 29 декабря 2005 г. № 447-ст);

5. Приложения

Перечень приложений к Стандарту

ОМЕР ОЖЕНИЯ	НАИМЕНОВАНИЕ ПРИЛОЖЕНИЯ	КРАТКОЕ ОПИСАНИЕ СОДЕРЖАНИЯ	ПРИМЕЧАНИЕ
1	Форма заявления на создание учетной записи пользователя	Содержит форму заявления, которое должен написать структурный руководитель пользователя для создания пользовательской учетной записи в ИС Поликлиники	Включено в настоящий документ
2	Форма заявления на создание и изменение полномочий пользователю	Содержит форму заявления, оформляемого структурным руководителем пользователя для наделения пользователя новыми полномочиями для работы с информационными ресурсами ИС Поликлиники	Включено в настоящий документ
3	Форма заявления на блокировку учетной записи пользователя	Содержит форму заявления, оформляемого структурным руководителем пользователя для блокирования учетной записи пользователя	Включено в настоящий документ
4	Форма заявления на создание нового информационного ресурса	Содержит форму заявления, оформляемого администратором существующего информационного ресурса для создания нового информационного ресурса	Включено в настоящий документ

Приложение 1.

Форма заявления на создание
учетной записи пользователя

ЗАЯВЛЕНИЕ

На создание (продление) учетной записи пользователя

создать (продлить) учетную запись пользователя:
отрудника, должность _____

_____

ационный ресурс: _____

компьютера _____ МАС-адрес _____
(заполняется при необходимости)

ами работы в информационной системе персональных данных АУЗРА «РСП» ознакомлен(а)
_____ _____ «___» _____ 20__г.
милия И.О. сотрудника) (подпись) (дата)

ание:
ист отдела кадров: _____ _____
(подпись) (ФИО)
«__»_____20__г.

- -

ьзователя: _____ Пароль: _____
группа: _____ Домен: _____
_____ IP-Адрес: _____
_____ Шлюз: _____
_____ DNS2: _____
_____ Пароль: _____
ервер: IP-адрес: _____ Порт: _____
_____ Пароль: _____

тратор информационной безопасности _____ «___» _____201_г.

- -

о
й администратор: _____ _____
(Подпись) (Фамилия И.О.)
Дата «___» _____201_г. Системное время ___ чч ___мм
- -

Приложение 2.

Форма заявления на изменение
полномочий

ЗАЯВЛЕНИЕ

На изменение полномочий пользователю

рошу изменить полномочия по работе с информационным ресурсом:

ИО сотрудника, должность ____

____

азвание запрашиваемого информационного ресурса: ______________________

нв.№ компьютера ______________ МАС-адрес ______________________

(заполняется при необходимости)

правилами работы в информационной системе персональных данных АУЗРА «РСП» ознакомлен(а)

__________________________ ______________ «___» __________ 20__ г.

(Фамилия И.О. сотрудника) (подпись) (дата)

Согласовано:

Специалист отдела кадров: ______________ ______________________

(подпись) (ФИО)

«__» ______________ 20__ г.

- -

Имя пользователя: ____________________ Пароль: ____________________

Рабочая группа: ____________________ Домен: ____________________

Имя ПК: ____________________ IP-Адрес: ____________________

Маска: ____________________ Шлюз: ____________________

DNS1: ____________________ DNS2: ____________________

E-mail: ____________________ Пароль: ____________________

Прокси-сервер: IP-адрес: ______________ Порт: ____________________

Логин: ____________________ Пароль: ____________________

Администратор информационной безопасности ______________ «__» __________ 201_ г.

- -

Выполнено

Системный администратор: ____________ ____________________

(Подпись) (Фамилия И.О.)

Дата «___» __________ 201_ г. Системное время ___ чч ___ мм

- -

Приложение 3.

Форма заявления на блокировку
учетной записи

ЗАЯВЛЕНИЕ

На блокировку учетной записи пользователя

Прошу заблокировать учетную запись:
ФИО сотрудника, должность ____
____
Учетная запись в системе:____
Название запрашиваемого информационного ресурса:_______________________________________

Срок действия полномочий прекратить с: "__" _____________ 20__г.
Обоснование блокировки:____
____
С гарантированным хранением данных в течении ____
(указывается срок хранения данных пользователя)

Согласовано:
Специалист отдела кадров:_____________ ____________________
(подпись) (ФИО)
«__»____________20__г.

Администратор информационной безопасности ___________ «__» _________201_г.

- -

Выполнено
Системный администратор: ___________ ______________________
(Подпись) (Фамилия И.О.)
Дата «___» _________201_г. Системное время ___ чч ___мм

- -

Приложение 4.

Форма заявления на создание
нового информационного ресурса
в рамках действующей ИС

СОГЛАСОВАНО

Владелец информационного актива "___" _____ 20__г.

Владелец информационного актива "___" _____ 20__г.
(при совместном владении информационным активом)

Сотрудник ответственный за ИБ "___" _____ 20__г.

ЗАЯВЛЕНИЕ

На создание нового информационного ресурса

Прошу создать новый информационный ресурс:

Наименование информационного ресурса	
Наименование ИС, в рамках которой создается информационный ресурс	
Назначение информационного ресурса	
Категория конфиденциальности	
Ф.И.О., должность, телефон ответственного (владельца) информационного ресурса	
Ф.И.О., должность, уровень полномочий привилегированных пользователей информационного ресурса	1. 2. ....

Обоснование служебной необходимости: _____

_____

_____

Ответственный (владелец) информационного ресурса

_____ _____ "___" _____ 20__г.
(Фамилия И.О. ответственного) (подпись) (дата)

Выполнено: _____
(системное имя информационного ресурса, описание выполненных действий)

Системный администратор _____ _____ Системное Время: _____ч____мм
(Подпись) (Фамилия И.О.)

Дата: "___" _____ 20__г.