УТВЕРЖДАЮ
Главный врач
НУЗ «Отделенческая больница
на ст. Белгород ОАО «РЖД»

_____ В.В. Болдырь
м.п.

«___» _____ 2015 г.

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
НУЗ «ОТДЕЛЕНЧЕСКАЯ БОЛЬНИЦА НА СТ. БЕЛГОРОД ОАО «РЖД»

Белгород 2015 г.

1. Общие положения

олитика информационной безопасности (далее – политика) определяет основные цели, направления, задачи и важнейшие принципы деятельности НУЗ «Отделенческая больница на ст. Белгород ОАО «РЖД» (далее - Учреждение) по вопросам защиты персональных данных.

Настоящая политика разработана с учетом положений Федерального закона Российской Федерации № 152-ФЗ «О персональных данных», Федерального закона Российской Федерации № 149-ФЗ «Об информационных технологиях и защите информации», Постановления Правительства Российской Федерации № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказа ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством российской федерации требований к защите персональных данных для каждого из уровней защищенности».

Политика основывается на соблюдении баланса интересов личности, общества и государства в информационной сфере и представляет собой совокупность управленческих решений, лежащих в основе организационно-распорядительных документов, регламентирующих правила и нормы обеспечения защиты персональных данных в процессе ее сбора, обработки, накопления и распространения.

За разработку, принятие и внедрение политики информационной безопасности отвечает руководитель Учреждения.

В организации назначаются работники, ответственные за реализацию политики безопасности персональных данных и поддержание ее в актуальном состоянии.

2. Термины и сокращения

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

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

Конфиденциальность персональных данных – обязательное для соблюдения Учреждением или иным получившим доступ к персональным данным юридическим или физическим лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Несанкционированный доступ (несанкционированные действия) (НСД) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Объект информатизации – совокупность информационных ресурсов содержащих персональные данные (ПДн), средств и систем обрабатывающих ПДн, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

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

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

Ресурс информационной системы – именованный элемент системного прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа и отношениями, регулируемыми нормативными правовыми актами.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. Система обеспечения безопасности персональных данных

Основными принципами, определяющими стратегию и тактику обеспечения безопасности персональных данных, являются соответственно концепция и *политика безопасности*.

Они определяют характер и направленность документов в области безопасности персональных данных, а также порядок *обеспечения безопасности персональных данных.*

Политика предусматривает:

– определение правового статуса и ответственности всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем при соблюдении законодательной базы в области обеспечения безопасности персональных данных;

– разработку механизма оперативного реагирования по фактам противоправных действий в отношении персональных данных, а также порядок ликвидации последствий этих действий и возмещения материального ущерба;

– разработку в рамках действующего законодательства мер дисциплинарного и административного воздействия на пользователей, работающих с

информационными ресурсами, при совершении ими противозаконных действий в отношении персональных данных;

– оценку эффективности применения действующего нормативно-методического обеспечения и разработку предложений по ее совершенствованию.

Необходимость разработки политики обусловлена важностью обеспечения режима безопасности не только на техническом, но и на управленческом уровне.

4. Цели и принципы обеспечения безопасности персональных данных

Основными *целями* политики являются:

– разработка и реализация корпоративной стратегии обеспечения защиты информационных ресурсов и технологий;

– оценка состояния безопасности ПДн, выявление внутренних и внешних угроз информационной безопасности, определение направлений предотвращения и нейтрализации этих угроз;

– координация и контроль деятельности элементов системы обеспечения безопасности персональных данных, выработка предложений по ее совершенствованию;

– создание условий для реализации прав граждан и организаций на разрешенную законом деятельность в информационной сфере;

– проведение единой технической политики в области обеспечения безопасности персональных данных.

Политика строится на *принципах*:

– соблюдения Конституции и законодательства Российской Федерации, норм международного права, нормативных правовых актов в области защиты информации;

– открытости в реализации функций управления хозяйственной деятельностью, предусматривающей информирование работников об основных аспектах и направлениях жизнедеятельности организации с учетом ограничений,

предусмотренных законодательством Российской Федерации в информационной сфере;

– правового равенства всех участников процесса информационного взаимодействия, если данное (поиск, получение, передача, производство и распространение информации) осуществляется любым законным способом;

– рассмотрения информационных ресурсов в качестве объектов собственности, введение которых в хозяйственный оборот осуществляется при соблюдении законных интересов их собственников, владельцев и распорядителей;

– учета того, что ограничение доступа к информации является исключением и вводится только на основании законов Российской Федерации, Указов Президента Российской Федерации, Постановлений Правительства, организационно-распорядительных документов организации и направлено на обеспечение защиты персональных данных или экономической безопасности;

– приоритетности использования при совершенствовании корпоративной информационной инфраструктуры современных конкурентоспособных отечественных информационных и телекоммуникационных технологий, технических и программных средств.

В основе политики лежат нормы:

– персональной ответственности за документирование персональных данных, определение грифа конфиденциальности, а также за его снятие;

– ограничения доступа к информации на основе норм, устанавливаемых федеральными законами и документами по защите информации;

– осуществления сбора, накопления и обработки конфиденциальной информации, в том числе данных о работниках (персональных данных) в соответствии с законодательством и внутренними документами по защите информации;

– централизованной разработки внутренних документов, регламентирующих вопросы безопасности персональных данных, обязательность их выполнения;

– единства технической политики в области реализации программно-технических мер по защите информационных технологий и ресурсов;

– обеспечения постоянного контроля состояния защиты персональных данных.

5. Защита информации на материальных носителях

Информация, содержащая ПДн, находящаяся на материальных носителях (бумажных, магнитных, оптических и т.п.), подлежит защите.

Документированная информация ПДн имеет отличительные реквизиты.

На документы или другие материальные носители информации персональных данных проставляется метка конфиденциальности.

Порядок регистрации, учета, оформления, тиражирования, хранения, использования и уничтожения конфиденциальных документов и других материальных носителей с конфиденциальной информацией, регламентируется внутренними нормативными документами.

Документы на материальных носителях, содержащие информацию с персональными данными, хранятся в сейфах, запираемых шкафах (ящиках). Специальные помещения, предназначенные для хранения конфиденциальных документов, в нерабочее время опечатываются.

Оборудование помещений должно исключать возможность несанкционированного проникновения и бесконтрольного пребывания в них посторонних лиц. Входные двери помещений оборудуются замками и устройствами для опечатывания.

Помещения, оборудованные охранной сигнализацией, могут не опечатываться.

Передача документированной информации с персональными данными по каналам факсимильной связи и сетям общего пользования без принятия мер по охране конфиденциальности информации запрещается.

Работникам, допущенным к информации с персональными данными, создаются следующие условия, обеспечивающие соблюдение ими установленного режима конфиденциальности:

– предоставление рабочего места в помещении, отвечающем требованиям обеспечения сохранности конфиденциальных документов;

– обеспечение сейфами (шкафами, ящиками) для хранения материальных носителей информации с персональными данными;

– установление на автоматизированные рабочие места средств защиты информации;

– обучение правилам обращения с персональными данными.

6. Защита персональных данных от утечки по техническим каналам

Одной из основных целей защиты персональных данных является предотвращение (существенное затруднение) несанкционированного съёма информации по всем возможным техническим каналам, которые могут иметь естественный характер или создаваться преднамеренно.

Защита конфиденциальной информации от утечки по техническим каналам представляет собой процесс, организуемый и поддерживаемый в организации с целью предупреждения и выявления каналов ее утечки.

Возможными каналами утечки информации являются:

– использование информативного акустического речевого излучения;

– использование виброакустических сигналов, возникающих при воздействии информативного речевого сигнала на строительные конструкции и инженерно – технические системы защищаемого помещения;

– прослушивание разговоров, ведущихся в защищаемом помещении, по информационным каналам общего пользования (городская телефонная сеть, сотовая, транкинговая и пейджинговая связь, радиотелефоны) за счет скрытого использования этих видов связи;

– использование электрических сигналов, возникающих в результате преобразования (микрофонного эффекта) информативного акустического сигнала в электрический, и распространяющихся по проводам и линиям передачи информации, выходящим за пределы контролируемой зоны;

– использование побочных электромагнитных излучения информативного сигнала от обрабатывающих персональные данные технических средств, в том числе возникающих за счет паразитной генерации, и излучения линий передачи информации;

– использование электрических сигналов, наводимых обрабатывающими конфиденциальную информацию техническими средствами и линиями передачи, на провода и линии передачи, выходящие за пределы контролируемой зоны;

– использование модулированного информативным сигналом радиоизлучения, возникающего при работе различных генераторов, входящих в состав технических средств установленных в защищаемом помещении, или при наличии паразитной генерации в узлах (элементах) таких технических средств;

– использование специальных электронных устройств съема речевой информации, тайно располагаемых в защищаемом помещении.

Защита конфиденциальной информации от утечки по техническим каналам должна подразумеваться на весь период работы субъекта с персональными данными, но может быть обеспечена организационными мерами, например, запретом на обсуждение сведений конфиденциального характера.

7. Защита персональных данных в автоматизированных системах и вычислительных сетях

Основным объектом защиты является информация, обрабатывающаяся и накапливающаяся в автоматизированных системах и вычислительных сетях организации.

Использование информационных ресурсов организации ведется только в производственных целях.

Информационные ресурсы идентифицируются и классифицируются. Порядок доступа к ним определяется их владельцами и регламентируется.

При определении прав доступа к информационным ресурсам следует руководствоваться должностными обязанностями работников и заключенными договорами о конфиденциальности.

7.1. Цели обеспечения безопасности персональных данных в автоматизированных системах и вычислительных сетях

Безопасность автоматизированных систем и вычислительных сетей обеспечиваются на всех стадиях их жизненного цикла с учетом роли всех вовлеченных в этот процесс сторон (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений и организаций).

Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты автоматизированных систем и вычислительных сетей осуществляются по согласованию с подразделением, ответственным за обеспечение информационной безопасности.

Ввод в эксплуатацию, эксплуатация и вывод из эксплуатации автоматизированных систем и вычислительных сетей в части вопросов информационной безопасности осуществляются при участии подразделения (работника), ответственного за обеспечение информационной безопасности.

В процессе эксплуатации автоматизированных систем и вычислительных сетей организации основной целью системы обеспечения безопасности персональных

данных является защита их от воздействий, связанных с имеющимися факторами риска, с целью минимизации потерь от их воздействия.

Это достигается путем:

– предотвращения кризисных ситуаций, способных нанести ущерб программным и аппаратным средствам, информации, а также персоналу;

– минимизации ущерба и быстрейшего восстановления программных и аппаратных средств, информации, пострадавших в результате кризисных ситуаций, расследование причин и принятие соответствующих мер.

Безопасность персональных данных реализуется с помощью средств защиты и управления защитой, средств контроля и регистрации, средств обеспечения безотказной работы и восстановления автоматизированных систем и вычислительных сетей.

В случае возникновения кризисных ситуаций, предотвращение которых средствами защиты невозможно, работа автоматизированных систем и вычислительных сетей осуществляется с применением мер обеспечения непрерывности их работы.

Ликвидация последствий кризисных ситуаций, расследование причин их возникновения и принятие мер осуществляется в установленном порядке.

7.2. Принципы обеспечения безопасности автоматизированных систем и вычислительных сетей на стадиях их жизненного цикла

В процессе создания автоматизированных систем и вычислительных сетей (определение требований заинтересованных сторон, анализ требований, техническое проектирование, реализация, интеграция и верификация, поставка, ввод в действие), обеспечивается:

– обоснованная формулировка требований к системам и сетям и их полноценная реализация;

– выбор оптимальных проектных решений;

– выбор адекватной модели жизненного цикла систем и сетей;

– разработка необходимой документации;

– приемка систем и сетей в эксплуатацию;

– предотвращение внесения недокументированных возможностей в системы и сети.

К разработке и вводу в эксплуатацию средств и систем защиты автоматизированных систем и вычислительных сетей организации, привлекаются на договорной основе организации, имеющие лицензии на данный вид деятельности в соответствии с законодательством Российской Федерации.

Средства защиты автоматизированных систем и вычислительных сетей и их компоненты сопровождаются весь срок их службы.

В случае невозможности выполнения этого требования для вновь разрабатываемых средств в договоре (контракте) оговаривается приобретение полного комплекта рабочей конструкторской документации, обеспечивающего возможность эксплуатации без участия разработчика.

При эксплуатации автоматизированных систем и вычислительных сетей в первую очередь обеспечивается защита от:

– несанкционированного доступа к информации, ее модификации или уничтожения;

– неумышленной модификации или уничтожения информации;

– недоставки или ошибочной доставки информации;

– отказа в обслуживании или ухудшения обслуживания;

– отказа от авторства сообщения.

В процессе сопровождения обеспечивается своевременное внесение изменений, необходимых для поддержки правильного функционирования и состояния автоматизированных систем и вычислительных сетей.

Не допустимо внесение изменений в автоматизированные системы и вычислительные сети, приводящих к нарушению их функциональности или появлению недокументированных возможностей.

На стадии вывода из эксплуатации отдельных элементов автоматизированных систем и вычислительных сетей из запоминающих устройств, обеспечивается удаление информации, используемой средствами обеспечения безопасности

персональных данных, а также информации, несанкционированное использование которой может нанести ущерб коммерческой деятельности организации.

Требования по безопасности персональных данных включаются во все договора и контракты на проведение работ или оказание услуг на всех стадиях жизненного цикла автоматизированных систем и вычислительных сетей, а также в соответствующую проектную документацию.

7.3. Меры по обеспечению безопасности персональных данных в автоматизированных системах и вычислительных сетях

Организационные меры по защите информации обеспечивают разработку, официальное оформление и доведение до исполнителей системы нормативно-методических документов, назначение ответственных за обеспечение информационной безопасности, а также организацию контроля соблюдения установленных правил и требований.

Прежде всего, обращается внимание на исключение возможности нарушения целостности и конфиденциальности обрабатываемой информации и обеспечивается запрет передачи конфиденциальной информации по открытым каналам связи без применения установленных мер по ее защите.

Обеспечивается использование вычислительных средств и информационных активов организации только в производственных целях.

Отдельно оговариваются права на использование работниками лицензируемых продуктов, приобретаемых организацией, и обязательства по порядку их использования и нераспространения.

Для повышения эффективности принимаемых мер наряду с организационными осуществляются технические меры по защите информации.

Они разрабатываются по результатам обследования объекта информатизации и оценки возможностей реализации замысла защиты на основе применения организационных мер, активизации встроенных механизмов используемых операционных систем и аппаратного обеспечения.

Технические меры защиты вычислительных систем и сетей осуществляются с учетом следующих основных принципов:

- обладания минимумом полномочий, необходимых и достаточных для решения пользователем своих задач;

- разделения информационной инфраструктуры на «контуры защиты». Защита организуется как внутри каждого контура, так и между смежными контурами. Информация определенной степени конфиденциальности, как правило, сосредотачивается внутри контура, а вход и выход за пределы контура контролируются.

В составе автоматизированных систем и вычислительных сетей (при необходимости) используются сертифицированные по требованиям безопасности и разрешенные к применению средства защиты информации.

Перечень используемых средств защиты информации согласуется с руководителем подразделения по защите информации организации.

Конкретные меры и способы обеспечения информационной безопасности, а также методы и способы использования средств защиты определяются особенностями конкретной вычислительной системы или сетевого оборудования и уточняются политиками информационной безопасности автоматизированных систем.

7.3.1. Защита серверного оборудования

Меры, принимаемые для защиты серверного оборудования, направляются на обеспечение конфиденциальности и целостности информационных ресурсов путем организации защиты вычислительных средств от несанкционированного доступа (среде выполнения вычислительного процесса, оперативной памяти и дисковому пространству), а также в помещения, где оно располагается.

Обеспечение доступности серверного оборудования достигается использованием средств мониторинга и диагностики, а также с помощью мер и средств обеспечения его безотказной работы.

7.3.2. Защита вычислительных сетей

Основной задачей защиты вычислительной сети организации является обеспечение доступности ресурсов сети и целостности передаваемой информации. Это обеспечивается:

– обеспечением целостности конфигурации сетей и контролируемого доступа к их ресурсам;

– затруднением перехвата внутреннего трафика;

– применением криптографических средств защиты информации, сертифицированных по требованиям безопасности информации в соответствии с действующим законодательством Российской Федерации, при передаче конфиденциальной информации по сетям общего пользования и вне контролируемых зон;

– организацией непрерывного управления и контроля состояния коммуникационного и сетеобразующего оборудования;

– исключением несанкционированного доступа в помещения, в которых располагается коммуникационное и сетеобразующее оборудование.

Для обеспечения доступа к сетям общего пользования (Internet и т.п.) применяются следующие первоочередные меры по защите внутренней сети:

– осуществление взаимодействия с сетью общего пользования через единый шлюз организации;

– обеспечение блокировки доступа к внутренним ресурсам рабочих мест и узлов, с которых осуществляется взаимодействие с сетью общего пользования, или выделение их в самостоятельную подсеть;

– использование сертифицированных криптографических средств защиты при передаче конфиденциальной информации по сети общего пользования;

– строгая регламентация и ограничение производственной необходимостью доступа работников организации к сети общего пользования.

7.3.3. Защита на уровне прикладных информационных систем

Основной задачей защиты ресурсов информационных систем является обеспечение их доступности и целостности, а также соблюдение установленных

требований обработки информации ограниченного доступа.

Меры защиты информационных систем должны предусматривать и регламентировать:

– доступ к информационным ресурсам;

– администрирование на прикладном и системно-техническом уровнях;

– авторизацию и разграничение доступа пользователей;

– аудит действий администраторов и пользователей;

– сопровождение программного обеспечения и поддержание его в актуальном состоянии.

7.3.4. Защита на уровне персональной ЭВМ

Защита персональной ЭВМ (ПЭВМ) является защитой рабочего места пользователя и одним из элементов комплексной защиты.

Меры защиты ПЭВМ должны предусматривать:

– исключение свободного доступа в помещения, где обрабатывается информация ограниченного доступа;

– ограничение возможности физического доступа с целью изменения конфигурации средств электронно-вычислительной техники (использование специальных защитных знаков, пломбирование, опечатывание и др.);

– исключение несанкционированной реконфигурации системного и прикладного программного обеспечения, а также самостоятельной его установки;

– исключение несанкционированного доступа к ресурсам ПЭВМ, на котором обрабатывается конфиденциальная информация;

– идентификацию и аутентификацию пользователя при запуске ПЭВМ;

– исключение возможностей несанкционированного просмотра конфиденциальной информации с монитора ПЭВМ, в том числе в отсутствие пользователя;

– исключения несанкционированного использования внешних носителей информации (магнитных и оптических дисков, карт памяти, фотоаппаратов, мобильных телефонов и т.п.), а также произвольных коммуникационных устройств;

– исключение возможности бесконтрольного изменения режима подключения ПЭВМ к вычислительным сетям, в том числе, к сетям общего пользования;

– антивирусную защиту ПЭВМ;

– обеспечение ведения системного журнала по основным событиям (журнала аудита).

7.4. Организация непрерывной работы автоматизированных систем и вычислительных сетей

Для обеспечения непрерывной работы и восстановления автоматизированных систем и вычислительных сетей в случае аварий, стихийных бедствий и других кризисных ситуаций предусматриваются соответствующие меры и средства.

7.4.1. Бесперебойное электропитание

Бесперебойное электропитание – наиболее важный элемент обеспечения непрерывной работы. Оно обеспечивается использованием системы резервного питания при выходе из строя основного источника, что позволяет сохранить работоспособность систем в течение известного времени.

При критичности автоматизированных систем к продолжительным авариям электросети для обеспечения бесперебойного электропитания могут использоваться автономные источники (дизель – генераторы).

7.4.2. Резервное копирование

Резервное копирование, предусматривающее хранение программного обеспечения и информационных массивов на внешних носителях, – основной способ обеспечения их сохранности.

Способ и периодичность резервного копирования регламентируется и определяется для каждой системы индивидуально.

Обеспечивается хранение несколько поколений данных. На каждую копию имеется дубликат, размещаемый отдельно от основной копии в специально оборудованном защищенном помещении, удаленном от резервируемой системы.

Организуется и регламентируется учет материалов резервного копирования.

7.4.3. Резервирование аппаратных ресурсов

Резервирование аппаратных ресурсов применяется для исключения нарушения работоспособности автоматизированных систем и вычислительных сетей.

Основным критерием целесообразности резервирования является степень критичности нарушения их работоспособности для обеспечения непрерывности деятельности организации, а также экономическая эффективность планируемых мероприятий.

7.4.4. Меры по обеспечению безотказной работы

Для предотвращения возникновения кризисных ситуаций, предусматриваются организационные мероприятия, направленные на предотвращение или снижение их отрицательного воздействия, которые включают в себя:

– локализацию области воздействия фактора риска;

– уведомление соответствующих должностных лиц о факте возникновения кризисной ситуации;

– предотвращение расширения кризисной ситуации, при необходимости, выведение из эксплуатации комплексов, систем или их отдельных компонентов;

– регламентирования процессов восстановления аппаратных, программных и информационных элементов автоматизированных систем и вычислительных сетей;

– расследование причин возникновения кризисной ситуации.

8. Обеспечение ответственности в сфере безопасности персональных данных

Действенность системы обеспечения безопасности персональных данных организации достигается установлением порядка, правил и зон ответственности в

сфере защиты информации, которые должны определять цели и содержание деятельности организации по обеспечению процессов управления информационной безопасностью.

8.1. Пути обеспечения доверия к персоналу

В организации для достижения поставленных целей и эффективного выполнения задач по обеспечению информационной безопасности определяется совокупность индивидуальных правил, устанавливающих допустимое взаимодействие между работником и объектами информатизации.

Правила персонифицируются для каждого работника в виде обязанностей с установлением ответственности за их исполнение. Формулировка обязанностей осуществляется с учетом установленного порядка обеспечения информационной безопасности. Ответственность за их надлежащее исполнение для каждого работника закрепляется в должностной инструкции.

Обязанности работника не должны быть критичными для организации с точки зрения последствий их неисполнения.

Обязанности работника не должны совмещать (в любой комбинации) функции разработки, сопровождения, исполнения, администрирования и контроля.

Исполнение обязанностей обеспечивается необходимыми ресурсами.

При приеме на работу проверяются: идентичность личности, заявляемая квалификация, точность и полнота биографических фактов, наличие рекомендаций.

Лица, которые принимаются на работу, связанную с доступом к защищаемым ресурсам, подвергаются оценке их профессиональной пригодности.

Проверка профессиональной компетенции принятых на работу осуществляется как на регулярной основе, так и внепланово при выявлении случаев нарушения ими требований информационной безопасности.

Все работники организации дают письменное обязательство о соблюдении режима коммерческой тайны. При этом условие о соблюдении режима коммерческой тайны должно распространяться на всю защищаемую информацию,

доверенную работнику или ставшую ему известной в процессе выполнения им своих служебных обязанностей.

Компетентность работников, обеспечивающих информационную безопасность, поддерживается на необходимом уровне существующей в организации системой переподготовки и повышения квалификации кадров.

8.2. Контроль выполнения режима защиты персональных данных

Контроль соблюдения режима защиты персональных данных в организации осуществляется с целью определения соответствия принятых мер по защите конфиденциальной информации, установленному режиму защиты персональных данных, выявления возможных каналов утечки и несанкционированного доступа к данной информации и принятию мер по их пресечению.

Контроль осуществляет подразделение по защите информации организации путем проведения плановых проверок или проверок по указанию руководителя организации состояния защиты персональных данных в подразделениях организации.

8.3. Ответственность за нарушение требований режима защиты персональных данных

Каждый работник организации, имеющий доступ к сведениям, содержащим персональные данные и иным, не подлежащим разглашению сведениям, несет дисциплинарную, материальную, административную, гражданско-правовую, уголовную ответственность, предусмотренную действующим законодательством Российской Федерации, за их разглашение и утрату, а также за нарушение установленного порядка обеспечения информационной безопасности. На руководителей подразделений организации возлагаются обязанности по обеспечению соблюдения установленного порядка обращения с информацией ограниченного доступа.

Работники обязаны:

- выполнять установленный порядок обращения с информацией ограниченного доступа;

- не разглашать информацию ограниченного доступа, в том числе и после прекращения трудового договора в течение срока, предусмотренного трудовым договором.

Работники организации, разгласившие информацию ограниченного доступа или нарушившие установленный порядок обращения с ней, а также работники, по вине которых произошла утрата конфиденциальных документов, несут ответственность, предусмотренную действующим законодательством Российской Федерации, внутренними документами организации и условиями трудового договора.

Описанная политика безопасности в практическом аспекте реализации представляет собой разрешительную систему доступа к информационным ресурсам.

Разрешительная система доступа пользователей к обрабатываемой информации в информационной системе персональных данных регулируется в соответствии с матрицей доступа путем соответствующих настроек компонент информационной системы обработки персональных данных.

9. Заключительные положения

9.1 Настоящая Политика вступает в силу с момента ее утверждения руководителем и действует до введения новой.

9.2 Ознакомление субъектов (сотрудников) с условиями настоящей Политики производится под подпись в листе ознакомления, являющемся ее неотъемлемой частью.

9.3 Подпись в листе ознакомления означает согласие и обязательство исполнения.