Приложение № 5
к приказу от 16 мая 2016 г. № 65

Политика
в отношении обработки информации и персональных данных в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Содержание

Определения

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность информации, в том числе персональных данных – состояние защищенности информации, в том числе персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации, в том числе персональных данных, при ее обработке в информационных системах.

Блокирование информации, в том числе персональных данных – временное прекращение обработки информации, в том числе персональных данных (за исключением случаев, если обработка необходима для уточнения информации).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на защищаемую информацию или ресурсы информационной системы.

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

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе.

Информационная система – совокупность содержащихся в базах данных информации, в том числе персональных данных, и обеспечивающих ее обработку информационных технологий и технических средств.

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

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность информации, в том числе персональных данных – обязательное для соблюдения оператором или иным получившим доступ к информации (персональным данным) лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы.

Нарушитель безопасности информации, в том числе персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации (персональных данных) при их обработке техническими средствами в информационных системах.

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

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка информации (персональных данных) – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией (персональными данными), включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации (персональных данных).

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющие обработку информации (персональных данных), а также определяющие цели обработки информации (персональных данных), состав информации (персональных данных), подлежащих обработке, действия (операции), совершаемые с информацией (персональными данными).

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

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

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

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.

Технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (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).

Угрозы безопасности информации (персональных данных) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации (персональным данным), результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации (персональных данных), а также иных несанкционированных действий при их обработке в информационной системе.

Уничтожение информации (персональных данных) – действия, в результате которых невозможно восстановить содержание информации (персональных данных) в информационной системе или в результате которых уничтожаются материальные носители информации (персональных данных).

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

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

Введение

Настоящая Политика в отношении обработки информации и персональных данных в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – Политика) разработана Областным государственным казенным учреждением здравоохранения «Новооскольская станция переливания крови» и определяет основные цели и задачи, а также общую стратегию построения системы защиты информации (далее - СЗИ) в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмент ГИС ЕИБД). Политика определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Политика разработана в соответствии с системным подходом к обеспечению информационной безопасности, который предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку СЗИ, с позиции комплексного применения технических и организационных мер и средств защиты информации (далее – СрЗИ).

Под информационной безопасностью защищаемой информации понимается защищенность информации в обрабатывающей ее инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам персональных данных) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности персональных данных (далее - ПДн), а также к прогнозированию и предотвращению таких воздействий.

Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности в сегменте ГИС ЕИБД, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации. Политика является методологической основой для:

- принятия управленческих решений и разработки практических мер по воплощению политики безопасности защищаемой информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз защищаемой информации;
- координации деятельности уполномоченных лиц при проведении работ по развитию и эксплуатации сегмента ГИС ЕИБД с соблюдением требований обеспечения безопасности защищаемой информации;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности защищаемой информации в сегменте ГИС ЕИБД.

Политика разработана на основании следующих документов:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждены руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662;
- Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) № 17 от 11 февраля 2013 года «Об утверждении Требований о защите информации, не

составляющей государственную тайну, содержащейся в государственных информационных системах».

В Политике определены требования к персоналу, работающему в сегменте ГИС ЕИБД, их степень ответственности и должностные обязанности, а также должностные обязанности работников, ответственных за обеспечение безопасности защищаемой информации в сегменте ГИС ЕИБД.

1 Общие положения

1.1 Целью настоящей Политики является обеспечение безопасности защищаемой информации в сегменте ГИС ЕИБД от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности информации.

1.2 Безопасность защищаемой информации достигается путем исключения несанкционированного, в том числе случайного доступа к защищаемой информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение защищаемой информации, а также иных несанкционированных действий.

1.3 Защищаемая информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности защищаемой информации.

2 Область действия

2.1 Требования настоящей Политики распространяются на всех работников, допущенных к работе в сегменте ГИС ЕИБД (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3 Система защиты информации

3.1 СЗИ, строится на основании:

- Перечня обрабатываемой информации и персональных данных в сегменте ГИС ЕИБД;
- Отчета об обследовании объекта Службы крови на соответствие требованиям по защите информации и персональных данных в сегменте ГИС ЕИБД (далее – Отчет об обследовании);
- Акта классификации сегмента ГИС ЕИБД;
- Акта определения уровня защищенности персональных данных, обрабатываемых в сегменте ГИС ЕИБД;
- Модели угроз и модели нарушителя безопасности информации, при ее обработке в сегменте ГИС ЕИБД (далее – Модель угроз);
- Технического задания на выполнение работ по развитию и обеспечению функционирования системы защиты персональных данных в сегменте ГИС ЕИБД;
- Руководящих документов ФСТЭК России и ФСБ России.

3.2 На основании этих документов определяется необходимый уровень защищенности информации, обрабатываемой в сегменте ГИС ЕИБД. На основании анализа актуальных угроз безопасности защищаемой информации, описанного в Отчете об обследовании и Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности защищаемой информации.

3.3 В зависимости от уровня защищенности сегмента ГИС ЕИБД и актуальных угроз, СЗИ может включать следующие подсистемы:

- идентификация и аутентификация субъектов доступа и объектов доступа (далее – ИАФ);
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей персональных данных;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение вторжений;

- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и информации;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- управление конфигурацией информационной системы и системы защиты персональных данных.

3.4 В список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки информации, операционными системами, прикладным программным обеспечением и специальными комплексами, реализующими СрЗИ.

4 Основные принципы построения СЗИ

4.1 Построение СЗИ сегмента ГИС ЕИБД и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

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

4.1.1 Законность.

4.1.1.1 Данный принцип предполагает осуществление защитных мероприятий и разработку СЗИ в соответствии с действующим законодательством в области защиты информации и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции. Работники и обслуживающий персонал сегмента ГИС ЕИБД должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту ПДн.

4.1.2 Системность.

4.1.2.1 Системный подход к построению СЗИ предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации сегмента ГИС ЕИБД. При создании СЗИ должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и несанкционированный доступ (далее – НСД) к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

4.1.3 Комплексность.

4.1.3.1 Комплексное использование методов и средств защиты информации предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей

слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

4.1.4 Непрерывность защиты информации.

4.1.4.1 Защита информации – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных СрЗИ, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла сегмента ГИС ЕИБД. Сегмент ГИС ЕИБД должен находиться в защищенном состоянии на протяжении всего времени своего функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода в незащищенное состояние. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

4.1.5 Своевременность.

4.1.5.1 Данный принцип предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите сегмента ГИС ЕИБД и реализацию мер обеспечения безопасности информации на ранних стадиях разработки в целом, и ее СЗИ, в частности. Разработка СЗИ должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

4.1.6 Преемственность и совершенствование.

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

4.1.7 Персональная ответственность.

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

4.1.8 Принцип минимизации полномочий.

4.1.8.1 Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено». Доступ к защищаемой информации должен предоставляться только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

4.1.9 Взаимодействие и сотрудничество.

4.1.9.1 Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность сегмента ГИС ЕИБД, для снижения вероятности возникновения негативных действий связанных с человеческим фактором. В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности ответственного за обеспечение безопасности информации и персональных данных и администратора ИБ.

4.1.10 Гибкость системы защиты информации.

4.1.10.1 Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

4.1.11 Простота применения средств защиты.

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

4.1.12 Научная обоснованность и техническая реализуемость.

4.1.12.1 Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации. СЗИ должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

4.1.13 Специализация и профессионализм.

4.1.13.1 Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информации, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация СрЗИ должна осуществляться профессионально подготовленными специалистами.

4.1.14 Обязательность контроля.

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

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

5 Требования к подсистемам СЗИ

5.1 СЗИ включает в себя следующие организационные и технические меры защиты информации, реализуемые в информационных системах в рамках ее системы обеспечения информационной безопасности, в зависимости от угроз безопасности, используемых информационных технологий и структурно-функциональных характеристик автоматизированной системы:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей персональных данных;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение вторжений;

– контроль (анализ) защищенности персональных данных;
– обеспечение целостности информационной системы и информации;
– обеспечение доступности персональных данных;
– защита среды виртуализации;
– защита технических средств;
– защита информационной системы, ее средств, систем связи и передачи данных;
– управление конфигурацией информационной системы и системы защиты персональных данных.

5.2 Подсистемы СЗИ имеют различный функционал в зависимости от уровня защищенности информации, обрабатываемой в сегменте ГИС ЕИБД.

5.2.1 Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

5.2.2 Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

5.2.3 Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

5.2.4 Меры по защите машинных носителей информации должны обеспечивать контроль доступа к машинным носителям информации и учет, контроль перемещения и использования.

5.2.5 Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

5.2.6 Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования защищаемой информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

5.2.7 Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

5.2.8 Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

5.2.9 Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

5.2.10 Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

5.2.11 Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам.

5.2.12 Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

5.2.13 Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

5.2.14 Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечить управление изменениями конфигурации информационной системы, анализировать потенциальное воздействие планируемых изменений в конфигурации информационной системы и системы защиты персональных данных, а также определению лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных.

6 Пользователи сегмента ГИС ЕИБД

6.1 В сегменте ГИС ЕИБД можно выделить следующие группы пользователей, участвующих в обработке и хранении защищаемой информации:

- администратора ИБ;
- ответственного за обеспечение безопасности информации и персональных данных;
- операторов (пользователей).

6.1.1 Администратор ИБ

6.1.1.1 Администратор ИБ ответственен за функционирование СЗИ, включая обслуживание и настройку административной, серверной и клиентской компонент.

6.1.1.2 Администратор ИБ обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении сегмента ГИС ЕИБД;
- обладает полной информацией о технических средствах и конфигурации сегмента ГИС ЕИБД;
- имеет доступ ко всем техническим средствам обработки информации и данным сегмента ГИС ЕИБД;
- обладает полной информацией о сегменте ГИС ЕИБД;
- имеет частичный доступ к СрЗИ и протоколирования и к части ключевых элементов сегмента ГИС ЕИБД.

6.1.1.3 Администратор ИБ уполномочен:

- реализовывать политики безопасности в части настройки средств криптографической защиты информации, межсетевых экранов и систем обнаружения атак, в

соответствии с которыми пользователь получает возможность работать с элементами сегмента ГИС ЕИБД;

- осуществлять аудит СрЗИ.

6.1.2 Ответственный за обеспечение безопасности информации и персональных данных

6.1.2.1 Ответственный за обеспечение безопасности информации и персональных данных обладает следующим уровнем доступа и знаний:

- должен знать законодательные и нормативные правовые акты, методические и нормативные материалы по вопросам, связанным с обеспечением информационной безопасности;
- должен знать порядок использования, обработки и хранения конфиденциальной информации, в том числе персональных данных, в информационных системах персональных данных.

6.1.2.2 Ответственный за обеспечение безопасности информации и персональных данных уполномочен:

- осуществлять внутренний контроль соблюдения законодательства Российской Федерации в части защиты информации, в том числе персональные данные ПДн;
- доводить до сведения работников положения законодательства Российской Федерации в части защиты информации, в том числе персональные данные ПДн;
- предоставлять необходимую информацию при проведении проверок регулирующими органами, а также проведении контрольных мероприятий по обеспечению информационной безопасности;
- организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов.

6.1.3 Операторы (пользователи) сегмента ГИС ЕИБД.

6.1.3.1 Оператор сегмента ГИС ЕИБД осуществляет обработку защищаемой информации. Обработка информации включает: возможность просмотра защищаемой информации, ручной ввод информации в систему сегмента ГИС ЕИБД, формирование справок и отчетов по информации, полученной из сегмента ГИС ЕИБД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗИ.

6.1.3.2 Оператор сегмента ГИС ЕИБД обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству защищаемой информации;
- располагает конфиденциальными данными, к которым имеет доступ.

7 Требования к персоналу по обеспечению защиты информации

7.1 Все работники, являющиеся пользователями сегмента ГИС ЕИБД, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемой информации и соблюдению режима безопасности информации.

7.2 При вступлении в должность нового работника, ответственный за обеспечение безопасности информации и персональных данных обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите информации, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования сегмента ГИС ЕИБД.

7.3 Работник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами сегмента ГИС ЕИБД и СЗИ.

7.4 Работники, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированного доступа к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

7.5 Работники, имеющие доступ к сегменту ГИС ЕИБД, должны следовать установленным процедурам поддержания режима безопасности информации при выборе и использовании паролей (если не используются технические средства аутентификации).

7.6 Работники, имеющие доступ к сегменту ГИС ЕИБД, должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности информации и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

7.7 Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

7.8 Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с сегментом ГИС ЕИБД, третьим лицам.

7.9 При работе с защищаемой информацией в сегменте ГИС ЕИБД работники обязаны обеспечить отсутствие возможности просмотра защищаемой информации третьими лицами с мониторов АРМ или терминалов.

7.10 При завершении работы в сегменте ГИС ЕИБД работники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

7.11 Работники должны быть проинформированы об угрозах нарушения режима безопасности информации и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на работников, которые нарушили принятые политику и процедуры безопасности ПДн.

7.12 Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы сегмента ГИС ЕИБД, могущих повлечь за собой угрозы безопасности информации, а также о выявленных ими событиях, затрагивающих безопасность информации, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности информации.

8 Должностные обязанности пользователей сегмента ГИС ЕИБД

8.1 Должностные обязанности пользователей сегмента ГИС ЕИБД описаны в следующих документах:

- инструкция администратора ИБ;
- инструкция пользователя СЗИ.

9 Ответственность пользователей сегмента ГИС ЕИБД

9.1 В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

9.2 Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

9.3 Администратор ИБ несет ответственность за все действия, совершенные от имени своих учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

9.4 При нарушениях работниками–пользователями сегмента ГИС ЕИБД правил, связанных с безопасностью информации, они несут ответственность, установленную действующим законодательством Российской Федерации.

Обозначения и сокращения

Администратор ИБ	– администратор информационной безопасности
АРМ	– автоматизированное рабочее место
АС	– автоматизированная система
ВПр	– вредоносная программа
ГИС	– государственная информационная система
Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
ИС	– информационная система
КЗ	– контролируемая зона
МЭ	– межсетевой экран
НСД	– несанкционированный доступ
ОС	– операционная система
ПДн	– персональные данные
ПО	– программное обеспечение
СЗИ	– система защиты информации
СрЗИ	– средство защиты информации
ЭВМ	– электронно-вычислительная машина