Приложение №27
к приказу
от «24» мая 2016 г. № 54Д

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ БАШКОРТОСТАН
«СТЕРЛИТАМАКСКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ»
(ГАПОУ РБ «Стерлитамакский медицинский колледж»)

УТВЕРЖДАЮ
Директор ГАПОУ РБ
«Стерлитамакский
медицинский колледж»
_____ В.Р.Ибрагимов
«24» 05 2016г.

ПОЛОЖЕНИЕ
об организации и обеспечении защиты персональных данных в государственном автономном профессиональном образовательном учреждении Республики Башкортостан «Стерлитамакский медицинский колледж»

Содержание

1. Назначение и область применения

1.1. Положение «Об организации и обеспечении защиты персональных данных» предназначено для организации и проведения мероприятий по обеспечению защиты персональных данных в государственном автономном профессиональном образовательном учреждении Республики Башкортостан «Стерлитамакский медицинский колледж» (далее – Учреждение) в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.2. Положение определяет порядок организации работ, требования, правила и рекомендации по обеспечению защиты персональных данных в Учреждении.

1.3. Положение является локальным правовым актом Учреждения. Требования Положения обязательны для выполнения всеми работниками, которые допущены к обработке персональных данных.

2. Термины и сокращения

АРМ	Автоматизированное рабочее место
БД	База данных
ВП	Вредоносная программа
ИС	Информационная система
ИСПДн	Информационная система персональных данных
ЛВС	Локальная вычислительная сеть
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
ПЭВМ	Персональная электронно-вычислительная машина
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
СЗПДн	Система (подсистема) защиты персональных данных
ФЗ	Федеральный закон

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

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 персональные данные или ресурсы информационной системы персональных данных.

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.

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

Информационная система персональных данных – 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 оператором

или иным получившим доступ к персональным данным 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.

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

Несанкционированный доступ (несанкционированные действия) – 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.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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 прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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

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

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

Средство 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.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

3. Общие положения

3.1. Необходимость проведения мероприятий по защите персональных данных в Учреждении определяется:

- Федеральным Законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей,

предусмотренных федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

– Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

3.2. Целью защиты ПДн является предотвращение возможной утечки информации и (или) несанкционированного и непреднамеренного изменения или разрушения ПДн.

3.3. Выполнение мероприятий по защите ПДн позволяет обеспечить защиту прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиту прав на неприкосновенность частной жизни, личную и семейную тайну.

3.4. Защита ПДн достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от несанкционированного доступа, программно-математических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также работоспособности технических средств.

3.5. Все работники, обрабатывающие ПДн и обеспечивающие защиту ПДн, должны быть ознакомлены с настоящим Положением под роспись.

3.6. Действие Положения не распространяется на устанавливаемый государственными органами режим защиты сведений, составляющих государственную тайну Российской Федерации.

4. Нормативные ссылки

4.1. Настоящее Положение разработано в соответствии с правовыми актами РФ:

– Федеральным Законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

– Федеральным Законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

– Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановлением Правительства Российской Федерации от 15.09.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

– «Базовой моделью угроз безопасности ПДн при их обработке в ИСПДн», утвержденной Заместителем директора ФСТЭК России 15.02.2008 г.

– «Методикой определения актуальных угроз безопасности ПДн при их обработке в ИСПДн», утвержденной Заместителем директора ФСТЭК России 15.02.2008 г.

– Приказ ФСТЭК России № 21 от 18 февраля 2013 года;

– «Методическими рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденными руководством 8 Центра ФСБ России 21.02.2008 г.

– «Типовыми требованиями 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», утвержденными руководством 8 Центра ФСБ России 21.02.2008 г.

5. Персональные данные, подлежащие защите

5.1. Персональные данные, подлежащие защите, утверждаются приказом руководителя Учреждения в виде «Перечня персональных данных, обрабатываемых в Учреждении.

5.2. Изменения, дополнения перечня персональных данных, обрабатываемых в Учреждении, осуществляются на основании информации, предоставляемой руководителями

подразделений, работники которых обрабатывают ПДн при выполнении должностных обязанностей.

5.3. Персональные данные, подлежащие защите в Учреждении, обрабатываются без использования средств автоматизации, а также в информационных системах персональных данных (ИСПДн).

6. Организационная система обеспечения безопасности ПДн

6.1. В состав организационной системы обеспечения безопасности ПДн Учреждения входят:

- руководитель Учреждения;
- руководители подразделений, работникам которых предоставлен доступ к ПДн;
- работники, которым предоставлен доступ к ПДн (пользователи ИСПДн).

6.2. Общее руководство организацией работ по защите ПДн осуществляет руководитель Учреждения.

6.3. Руководство и контроль за обеспечением безопасности ПДн при обработке в ИСПДн, организацию работ по разработке документации по защите ПДн, разработке СЗПДн, по проведению организационных и технических мероприятий по защите ПДн осуществляет ответственный за организацию обработки персональных данных.

6.4. Из состава работников Учреждения назначается ответственный за обеспечение безопасности персональных данных. Права и обязанности работника, ответственного за обеспечение безопасности персональных данных (администратора безопасности), включаются в его должностные обязанности.

6.5. Работники, которым предоставлен доступ к ПДн в рамках обработки без использования средств автоматизации, непосредственно реализуют организационные меры по обеспечению сохранности носителей ПДн и выполнения процедур по соблюдению требований законодательства.

6.6. Пользователи ИСПДн непосредственно реализуют требования безопасности информации, принятые для ИСПДн, исполняют установленные режимы защиты ПДн, обеспечивают строгое исполнение предписанных правил безопасности информации.

7. Защита ПДн при обработке без использования средств автоматизации

7.1. Требования к обеспечению безопасности персональных данных при их обработке без использования средств автоматизации установлены Постановлением Правительства РФ от 15.09.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

7.2. Данный вид обработки ПДн (а также состав ПДн и перечень лиц, допущенных к обработке) указывается в Перечне обрабатываемых персональных данных и Перечне подразделений и должностных лиц, допущенных к работе с персональными данными.

7.3. Защита ПДн, обрабатываемых без использования средств автоматизации, обеспечивается выполнением следующих мероприятий:

- определением мест хранения персональных;
- обеспечением раздельного хранения персональных данных;
- соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним.

7.4. Носители ПДн подлежат уничтожению по достижении целей обработки и/или в случае утраты необходимости в их хранении. Уничтожение носителей осуществляется подразделением, в котором осуществлялось хранение носителя с участием работников подразделения, из которого поступил носитель.

7.5. В случаях истечения срока хранения (архивного хранения) носителей ПДн осуществляется уничтожение и/или обезличивание ПДн при наличии такой возможности в порядке, предусмотренном Правилами обработки, хранения и уничтожения персональных данных в Учреждении.

8. Защита ПДн при обработке в информационных системах персональных данных

8.1. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

– определение угроз безопасности персональных данных при их обработке в ИСПДн, формирование на их основе модели угроз;

– организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

– обеспечение сохранности носителей персональных данных;

– утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

– использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

– назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе;

– оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– учет машинных носителей персональных данных;

– обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

– восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных;

– обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

– контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

– разработку на основе модели угроз и модели нарушителя системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

– установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

– обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

8.2. Модель угроз безопасности персональных данных при их обработке в специальных информационных системах персональных данных разрабатывается с использованием методических документов ФСТЭК России и (или) ФСБ России. Результаты определения и оценки актуальных угроз безопасности ПДн при их обработке в ИСПДн Учреждения утверждаются руководством Учреждения.

8.2.1. Выявление угроз безопасности ПДн, реализуемых с применением программных и программно-аппаратных средств, осуществляется на основе экспертного метода, в том числе путем опроса специалистов по информационным технологиям, персонала ИСПДн, при этом могут использоваться специальные инструментальные средства (сетевые сканеры) для подтверждения наличия и выявления уязвимостей программного и аппаратного обеспечения ИСПДн. Для проведения опроса могут составляться специальные опросные листы.

8.2.2. При необходимости применения (в случае передачи ПДн по незащищенным каналам связи) средств криптографической защиты информации для ИСПДн разрабатывается

Модель нарушителя безопасности персональных данных. Модель нарушителя разрабатывается на основе «Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных» ФСБ России. На основе разработанной модели нарушителя для ИСПДн определяется уровень криптографической защиты ПДн, которому должны соответствовать применяемые средства криптографической защиты.

8.3. Требования к обеспечению безопасности ПДн при их обработке в ИСПДн

8.3.1. Разрешительная система допуска пользователей к информационным ресурсам

8.3.1.1. Разграничение доступа к информационным ресурсам, содержащим ПДн, должно осуществляться на основании «Перечня должностей Учреждения, замещение, которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным».

8.3.1.2. На периодической основе или после каждого изменения в ИСПДн ответственный за обеспечение безопасности персональных данных должен проводить проверку соответствия прав пользователей, определенных «Перечнем должностей Учреждения, замещение, которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным».

8.3.2. Регистрация действий пользователей

8.3.2.1. Регистрация действий пользователей должна осуществляться средствами системного программного обеспечения и СЗИ ИСПДн.

8.3.2.2. Подлежат обязательной регистрации следующие операции, осуществляемые в ИСПДн:

- регистрация входа (выхода) пользователей в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова.
- регистрация выдачи печатных (графических) документов на бумажный носитель;
- регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных;
- регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа.

8.3.3. Обеспечение безопасности при хранении носителей информации ПДн

8.3.3.1. Подлежат учету следующие защищаемые носители ПДн:

- накопители на жестких магнитных дисках, установленные в серверы ИСПДн;
- накопители на жестких магнитных дисках, установленные в АРМ, на которых предусмотрено хранение ПДн;
- накопители для хранения резервных копий;
- внешние носители ПД (дискеты, компакт-диски, flash-накопители), на которых технологией обработки ПДн разрешается хранение или передача ПДн.

8.3.3.2. Учет защищаемых носителей информации должен осуществляться в Журналах учета машинных носителей в соответствии с порядком, предусмотренным «Правилами обработки, хранения и уничтожения персональных данных в Учреждении.

8.3.3.3. Обязанность по ведению учета электронных носителей ПДн возлагается на ответственного за обеспечение безопасности персональных данных.

8.3.3.4. В случае смены владельца или назначения, списания и выведения из эксплуатации защищаемых носителей информации необходимо обеспечить уничтожение ПДн с носителей. Уничтожение информации с носителей информации должно осуществляться путем многократной записи информации на носители и/или путем физического уничтожения носителя.

8.3.3.5. По факту уничтожения носителя ПДн должен составляться соответствующий Акт, в порядке, предусмотренном Правилами обработки, хранения и уничтожения персональных данных в Учреждении.

8.3.4. Резервирование технических средств, дублирование массивов и носителей информации.

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации приведен в Приложении А.

8.3.4.1. Обеспечение целостности и доступности ПДн, программных и аппаратных средств ИСПДн, а также средств защиты, при их случайной или намеренной модификации, должно осуществляться с помощью резервного копирования (дублирования массивов и носителей информации) обрабатываемых данных, резервирования элементов ИСПДн.

8.3.4.2. Для обеспечения целостности ИСПДн должны выполняться следующие мероприятия по резервированию:

– резервные копии информационных ресурсов, содержащих ПДн, должны храниться в специально выделенном месте, территориально отдаленном от места обработки самой информации;

– для обеспечения сохранности резервных копий должен быть применён комплекс организационных и физических мер защиты от НСД;

– носители, на которые осуществляется резервное копирование, должны регулярно проверяться на отсутствие повреждений, сбоев логической структуры, файловой системы;

– должны проводиться регулярные проверки процедур восстановления данных.

8.3.5. Использование средств защиты информации

В соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» для обеспечения уровня защищенности персональных данных при их обработке в информационных системах необходимо использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

При использовании средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия (сертификацию), должны выполняться следующие мероприятия:

– установка и ввод в эксплуатацию средств защиты информации осуществляется в соответствии с эксплуатационной и технической документацией;

– проведение обучения лиц, использующих средства защиты информации, правилам работы с ними;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним. Форма журнала учета средств защиты информации, эксплуатационной и технической документации к ним приведена в Приложении 1. Форма журнала учета средств криптографической защиты информации, эксплуатационной и технической документации к ним приведена в Приложении 2;

– контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– периодическое тестирование средств защиты в соответствии с эксплуатационной документацией на СЗИ. Форма журнала проведения периодического тестирования СЗИ приведена в Приложении 3;

– разбирательство и составление заключений по фактам несоблюдения условий использования средств защиты информации, которые могут привести к нарушению целостности, конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

8.3.6. Использование защищенных каналов связи

8.3.6.1. При взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) основными методами и способами защиты информации от несанкционированного доступа являются:

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

– обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;

– анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);

– защита информации при ее передаче по каналам связи;

– использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;

– использование средств антивирусной защиты;

– централизованное управление системой защиты персональных данных информационной системы.

8.3.6.2. Для обеспечения безопасности персональных данных при удаленном доступе к информационной системе через информационно-телекоммуникационную сеть международного информационного обмена дополнительно должны применяться следующие основные методы и способы защиты информации от несанкционированного доступа:

– проверка подлинности отправителя (удаленного пользователя) и целостности, передаваемых по информационно-телекоммуникационной сети международного информационного обмена данных;

– управление доступом к защищаемым персональным данным информационной сети;

– использование атрибутов безопасности.

8.3.6.3. Для обеспечения безопасности персональных данных при межсетевом взаимодействии отдельных информационных систем через информационно-телекоммуникационную сеть международного информационного обмена должны применяться следующие основные методы и способы защиты информации от несанкционированного доступа:

– создание канала связи, обеспечивающего защиту передаваемой информации;

– осуществление аутентификации взаимодействующих информационных систем, и проверка подлинности пользователей и целостности передаваемых данных.

8.3.6.4. Защита каналов связи реализуется следующими организационно-техническими способами:

– Размещение линий связи и сетевого оборудования в пределах контролируемой зоны (КЗ);

– Использование волоконно-оптических линий связи, затрудняющих или исключающих возможность перехвата передаваемой информации;

– Использование средств криптографической защиты.

8.3.7. Физическая защита помещений и технических средств

8.3.7.1. Размещение ИСПДн и охрана помещений, в которых ведется работа с персональными данными, должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

8.3.7.2. Выполнение требований по исключению возможности неконтролируемого проникновения или пребывания в помещениях ИСПДн посторонних лиц реализуется осуществлением организационных и технических мер по созданию контролируемой зоны (КЗ) Учреждения.

8.3.7.3. Границами КЗ являются:

– периметр охраняемой территории Учреждения;

– ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории;

– стены помещений Учреждения.

8.3.7.4. В состав КЗ должны входить:

– помещения, в которых размещены рабочие станции, серверы, сетевое оборудование, входящие в состав ИСПДн;

– помещения, в которых проходят кабельные линии связи ИСПДн;

– помещения, в которых хранятся бумажные носители ПДн (архивы, помещения работников Учреждения).

8.3.7.5. Размещение технических средств, обрабатывающих ПДн, должно осуществляться с учетом требования минимизации доступа в рабочие помещения лиц, не связанных с обработкой ПДн и обслуживанием оборудования.

8.3.7.6. Доступ посторонних лиц (посетителей, работников обслуживающих организаций) в контролируемую зону в рабочее время осуществляется только в сопровождении работников Учреждения.

8.3.7.7. Размещение устройств отображения и печати информации, используемых в составе ИСПДн, должно осуществляться с учетом максимального затруднения визуального просмотра информации посторонними лицами.

8.3.7.8. Серверы и коммуникационное оборудование ИСПДн должны располагаться в отдельном помещении или в металлических шкафах с прочной запираемой дверью. Ключи от дверей помещений и шкафов должны быть только у лиц, имеющих право доступа в них.

8.3.7.9. В нерабочее время доступ в контролируемую зону должен быть исключен следующими мерами:

- организация и обеспечение контроля доступа в помещения работников и посетителей в рабочие дни с 09.00 до 18.00.
- организация и обеспечение охраны помещений в рабочие дни с 18.00 до 09.00, а также в выходные и праздничные дни.
- не допускать проникновения и пребывания посторонних лиц в помещениях в рабочие дни с 17.00 до 09.00, а также в выходные и праздничные дни. При необходимости использования помещений в указанное время, допуск в помещения осуществляется по письменной заявке ответственным лицом.
- внос и вынос материальных ценностей в помещения и из помещений осуществляется только в присутствии ответственного лица.

8.3.8. Использование средств антивирусной защиты

8.3.8.1. Средства антивирусной защиты предназначены для реализации следующих функций:

– антивирусное сканирование;

– блокирование вредоносных программ;

– автоматизированное обновление антивирусных баз;

– ограничение прав пользователя на изменение настроек антивирусного программного обеспечения;

– автоматический запуск сразу после загрузки операционной системы.

8.3.8.2. Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

8.3.8.3. Обо всех случаях сбоев антивирусного программного обеспечения (появления сообщений об ошибках) пользователь должен немедленно уведомлять

ответственного за обеспечение безопасности персональных данных.

8.3.9. Обеспечение внешней защиты персональных данных.

8.3.9.1. Пропускной режим в Здании Учреждения не осуществляется.

8.4. Порядок разработки, ввода в действие и эксплуатации СЗПДн

8.4.1.1. Требования по защите ПДн для каждой ИСПДн должны формироваться в виде Технического задания на создание СЗПДн в ИСПДн на этапе разработки (модернизации) ИСПДн.

8.4.1.2. Требования должны формироваться на основании положений руководящих документов ФСТЭК России и ФСБ России, перечень которых приведен в п. 4.1.

8.4.1.3. Для вновь создаваемых ИСПДн, а также для функционирующих ИСПДн, не включающих в себя СЗПДн проводятся следующие мероприятия:

– обследование ИСПДн и разработка технического (частного технического) задания на создание СЗПДн;

– проектирование и реализация ИСПДн и СЗПДн в её составе;

– ввод в действие СЗПДн, включающее опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

8.4.1.4. Для функционирующих ИСПДн, включающих в себя СЗПДн, доработка (модернизация) СЗПДн должна проводиться в случае, если:

– изменился состав обрабатываемых ПДн;

– изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ЛВС ИСПДн) или технологический процесс обработки ПДн, вследствие которого произошли изменения в структуре ИСПДн;

– изменился состав угроз безопасности ПДн в ИСПДн;

– изменился уровень защищенности (класс) ИСПДн.

8.5. Порядок оценки соответствия ИСПДн требованиям безопасности ПДн

8.5.1.1. Оценка соответствия ИСПДн требованиям безопасности ПДн проводится в виде внутренней оценки соответствия / добровольной аттестации на соответствие требованиям безопасности информации.

8.5.1.2. Для ИСПДн, оценка соответствия которых проводится в виде внутренней оценки соответствия, необходимо выполнять следующие требования:

– оценка соответствия осуществляется на основе собственных доказательств или на основании доказательств, полученных с участием привлеченных организаций, имеющих необходимые лицензии;

– в случае проведения оценки на основе собственных доказательств Учреждения самостоятельно формирует комплект документов, таких как техническая документация, другие документы и результаты собственных исследований, послужившие мотивированным основанием для подтверждения соответствия информационной системы персональных данных всем необходимым требованиям;

– результаты оценки соответствия должны содержать:

- наименование и местонахождение ИСПДн;
- информацию об объекте подтверждения соответствия;
- наименование документов, на соответствие требованиям, которых оценивается ИСПДн;
- сведения о принятых мерах по обеспечению соответствия ИСПДн необходимым требованиям;
- сведения о документах, послуживших основанием для подтверждения соответствия ИСПДн требованиям;
- срок действия оценки соответствия и условия повторной оценки.

8.5.1.3. Добровольная аттестация ИСПДн на соответствие требованиям безопасности информации проводится в соответствии с Положением по аттестации объектов информатизации по требованиям безопасности информации, утвержденным председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994 г.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

Аттестация проводится органом по аттестации в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации из следующего основного перечня работ:

- анализ исходных данных по аттестуемому объекту информатизации;
- предварительное ознакомление с аттестуемым объектом информатизации;
- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;
- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

Органы по аттестации аккредитуются ФСТЭК России с выдачей лицензии на проведение работ по аттестации объектов информатизации.

Аттестационные испытания проводятся в соответствии с разработанной Программой и методикой проведения аттестационных испытаний. По результатам испытаний оформляются заключение с подтверждающими протоколами, а также, в случае положительного заключения, выдается аттестат соответствия.

9. Требования к персоналу по обеспечению защиты ПДн

9.1. При вступлении в должность нового работника непосредственный руководитель структурного подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн. Ответственный за обеспечение безопасности персональных данных обучает навыкам выполнения процедур, необходимых для работы в ИСПДн и выполнения требований по защите ПДн и знакомит под роспись с Инструкцией пользователя информационных систем персональных данных.

9.2. Работники должны соблюдать установленные организационно-распорядительными документами требования по режиму обработки персональных данных, учету, хранению, передаче носителей информации и обеспечению безопасности ПДн.

9.3. Работники должны быть проинформированы об ответственности за нарушение требований по обеспечению безопасности ПДн.

10. Контроль состояния защиты ПДн

10.1. Целью контроля состояния защиты является своевременное выявление и предотвращение утечки информации.

10.2. Контроль состояния защиты ПДн должен осуществляться ежегодно в соответствии с утвержденным Планом внутренних проверок состояния защиты персональных данных. Форма журнала учета проведения мероприятий приведена в Приложении 4.

10.3. Проведение контроля состояния защиты включает в себя мероприятия по оценке:

- соблюдения требований руководящих и нормативно-методических документов по защите ПДн;

– работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;

– знаний и выполнения персоналом своих функциональных обязанностей в части защиты ПДн.

10.4. Проверка проводится дополнительно при изменении состава технических средств и систем, условий обработки информации, содержащей ПДн.

10.5. В случаях обнаружения нарушений при обработке ПДн в ИСПДн необходимо:

– немедленно прекратить обработку ПДн в ИСПДн, где обнаружены нарушения и принять меры к их устранению;

– организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц.

10.6. Возобновление работ разрешается только после устранения нарушений и проверки достаточности и эффективности принятых мер, соответствия их требованиям нормативных документов по защите ПДн.

Приложение А. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации.

1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.
2. К использованию, для создания резервной копии в ИСПДн, допускаются только зарегистрированные в журнале учета носители.
3. Ответственный за обеспечение безопасности персональных данных обязан осуществлять периодическое резервное копирование персональных данных, обрабатываемых в ИСПДн.
4. Носители информации (ЖМД, ГМД, CD-ROM, USB накопитель, другие), предназначенные для создания резервной копии и хранения ПДн выдаются установленным порядком ответственным за организацию обработки ПДн или ответственным за обеспечение безопасности персональных данных. По окончании процедуры резервного копирования электронные носители ПДн сдаются на хранение ответственному за обеспечение безопасности персональных данных, или руководителю подразделения, или ответственному за организацию обработки ПДн.
5. Перед резервным копированием пользователь или ответственным за обеспечение безопасности персональных данных обязан проверить электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель) на отсутствие вирусов.
6. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль в соответствии с разделом 16 настоящего Положения.
7. Запрещается запись посторонней информации на электронные носители (ЖМД, ГМД, CD-ROM, USB накопитель и другие) резервной копии.
8. Порядок создания резервной копии:
- вставить в компьютер зарегистрированный электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель, другие) для резервного копирования;
- выбрать необходимый каталог (файл) для создания резервного архива;
- при использовании систем управления базами данных необходимо создать файл с резервной копией защищаемой информации с помощью встроенных средств системы;
- выполнить процедуру создания резервной копии;
- произвести копирование на отчуждаемый носитель;
- произвести отключение отчуждаемого носителя и, создав не обходимые записи в журналах убрать носитель в хранилище.
9. Хранение отчуждаемого носителя с резервной копией защищаемой информации осуществляется в запираемом шкафу или сейфе совместно с ключевой и аутентифицирующей информацией.
10. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.
11. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется ответственным за обеспечение безопасности персональных данных в специальном хранилище.
12. При необходимости ремонта технических средств, с них удаляются опечатывающие

пломбы и по согласованию с ответственным за обеспечение безопасности персональных данных оборудование передается в сервисный центр производителя. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации. Работа с использованием неисправных технических средств запрещается.

13. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и(или) защищаемой информации в результате сбоев в сети электропитания.

14. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных.

15. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся у ответственного за обеспечение безопасности персональных данных. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

16. Ответственность за проведение резервного копирования в ИСПДн в соответствии с требованиями настоящего Положения возлагается на пользователя ИСПДн и ответственного за обеспечение безопасности персональных данных.

17.Ответственность за проведение мероприятий по восстановлению работоспособности технических средств, средств защиты информации (далее – СЗИ) и программного обеспечения баз данных возлагается на ответственного за обеспечение безопасности персональных данных.

Приложение 1. Форма Журнала учета средств защиты информации, эксплуатационной и технической документации к ним

Журнал учета средств защиты информации,
эксплуатационной и технической документации к ним

Журнал начат «____» _____ 201__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 201__ г.
Должность
_____ / ФИО должностного лица /

№ п/п	Наименование СЗИ	Серийный (заводской) номер СЗИ	Организация, выполнявшая установку СЗИ	Место установки СЗИ	Примечание
1					
2					
3					
4					
5					

Приложение 2. Форма Журнала учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

Журнал учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

Журнал начат «____» _____ 201__ г.

_____ / ФИО должностного лица /

Журнал завершен «____» _____ 201__ г.

_____ / ФИО должностного лица /

№	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Примечание
				От кого получены	Дата и номер сопроводительного письма	ФИО пользователя СКЗИ	Дата и расписка в получении	ФИО сотрудника, проводившего установку	Дата установки и подписи лиц, произведших установку	Номера аппаратных средств, в которые установлены СКЗИ	
1	2	3	4	5	6	8	9	10	11	12	13
1.											
2.											
3.											
4.											

Приложение 3. Форма Журнала периодического тестирования средств защиты информации

Журнал периодического тестирования средств защиты информации

Журнал начат «____» _____ 201__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 201__ г.
Должность
_____ / ФИО должностного лица /

№ п/п	Наименование СЗИ/СКЗИ	Регистрационные номера СЗИ/СКЗИ	Дата проведения тестирования	ФИО и подпись проводившего тестирование	Вид теста и используемые средства для его проведения	Результат тестирования (успешный/неуспешный), примечания	Дата проведения следующего тестирования
1							
2							
3							
4							
5							

Приложение 4. Форма Журнала учета мероприятий по защите информации

Журнал учета мероприятий по защите информации

Журнал начат «____» _____ 201__ г.

_____ / ФИО должностного лица /

Журнал завершен «____» _____ 201__ г.

_____ / ФИО должностного лица /

№ п/п	Наименование мероприятия	Краткое описание мероприятия	**Дата проведения** мероприятия	**ФИО проводившего** мероприятие	**Подпись проводившего** мероприятие	Примечание
1						
2						
3						
4						
5						