УТВЕРЖДЕНО
Приказом ГБУЗ СК «Городская детская
поликлиника №3» города Ставрополя
№ _____ от «___» _____ 2014 г.

РЕГЛАМЕНТ
обеспечения безопасности персональных данных ГБУЗ СК «Городская детская поликлиника №3» города Ставрополя

г. Ставрополь 2014

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники
Блокирование персональных данных	Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
Доступ к персональным данным	Возможность получения персональных данных и их использования
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Конфиденциальность информации	Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
Несанкционированный доступ (несанкционированные действия)	Доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам
Носитель персональных данных	Бумажный или машинный носитель информации, содержащий персональные данные, например: бумажные документы, магнитные диски, магнитные ленты, CD/DVD, USB-флэш диски и т.п.)
Обработка персональных данных	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных
Персональные данные (ПДн)	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Предоставление персональных данных	действия, направленные на получение персональных данных определенным кругом лиц или передачу персональных данных определенному кругу лиц
Средство защиты информации	Техническое и (или) программное средство, предназначенное или используемые для защиты информации
Технические средства информационной системы персональных данных	Средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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 персональных данных	Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных
Уничтожение персональных данных	Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных
Целостность информации	Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

СОКРАЩЕНИЯ

ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
СЗПДн	Система защиты персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Регламент определяет порядок проведения мероприятий по обеспечению безопасности персональных данных в ГБУЗ СК «Городская детская поликлиника №3» города Ставрополя (далее – Учреждение), а также права, обязанности и ответственность работников Учреждения по выполнению указанных мероприятий.

Настоящий Регламент разработан в соответствии с требованиями следующих нормативно-правовых актов:

- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Область действия настоящего документа включает в себя:

- все процессы обработки персональных данных в Учреждении, как с использованием средств автоматизации, так и без использования таковых;
- все информационные системы Учреждения, в которых осуществляется обработка персональных данных.

В Учреждении выделены три категории работников, участвующих в обеспечении безопасности персональных данных (далее – ПДн):

Администраторы ИСПДн (Ответственные за администрирование информационных систем персональных данных) – работники Учреждения, обеспечивающие бесперебойное функционирование информационных систем персональных данных;

Администраторы ИБ (Ответственные за обеспечение безопасности ПДн) – работники Учреждения, обеспечивающие функционирование системы защиты персональных данных;

Пользователи – работники Учреждения, непосредственно осуществляющие обработку персональных данных.

2. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обеспечение безопасности персональных данных при их обработке в Учреждении обеспечивается построением Системы защиты персональных данных (далее - СЗПДн).

Функционирование СЗПДн обеспечивается комплексом организационных мероприятий, а также применением технических средств защиты информации от несанкционированного доступа и программно-технических воздействий с целью нарушения конфиденциальности, целостности (модификации, уничтожения) и доступности ПДн в процессе их обработки, передачи и хранения.

Объектом защиты СЗПДн являются информационные системы персональных данных, носители ПДн (бумажные и машинные), а также помещения, в которых производится обработка ПДн.

Мероприятия по защите ПДн от несанкционированного доступа и и других неправомерных воздействий (далее – НСД) реализуются в рамках следующих подсистем СЗПДн:

- подсистема управления доступом;
- подсистема регистрации и учета;
- подсистема обеспечения целостности;
- подсистема антивирусной защиты;
- подсистема межсетевого экранирования;
- подсистема анализа защищенности;
- подсистема обнаружения вторжений;
- подсистема физической защиты.

Все средства защиты информации, применяемые в составе СЗПДн, должны пройти оценку соответствия в порядке, установленном Законодательством РФ.

3. ПОДСИСТЕМЫ ЗАЩИТЫ СЗПДН

3.1. Подсистема управления доступом

В подсистеме управления доступом реализуются следующие мероприятия по обеспечению безопасности ПДн:

- использование разрешительной системы допуска работников Учреждения к обработке ПДн;
- разграничение прав доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации с помощью встроенных функций операционной системы, прикладных систем обработки ПДн либо специализированных средств защиты информации;
- применение средств парольной защиты для идентификации и аутентификации пользователей ПДн в ИСПДн Учреждения, осуществляемое Администратором ИСПДн в соответствии с указанными ниже требованиями.

Требования к настройке и применению средств парольной защиты:

- при создании новой или реинициализации уже существующей учётной записи пользователя для неё должен устанавливаться стартовый пароль, который пользователь обязан изменить при первом входе в систему;
- срок действия персонального пароля должен составлять 90 дней. В случае, если пользователь не произвел смену пароля до истечения установленного срока, его учетная запись блокируется;
- после совершения 5 неудачных попыток ввода пароля учетная запись пользователя автоматически блокируется на 30 минут. При этом неудачные попытки прохождения аутентификации пользователя должны регистрироваться в системном журнале;
- при создании или изменении пароля должна выполняться автоматическая проверка соблюдения следующих условий:
  - пароль не должен содержать имя учетной записи пользователя или какую-либо его часть;
  - пароль должен состоять не менее чем из восьми символов;
  - в пароле должны присутствовать символы из всех перечисленных категорий:
    - прописные буквы английского алфавита от A до Z;
    - строчные буквы английского алфавита от a до z;
    - десятичные цифры (от 0 до 9);
    - специальные символы (например, !, $, #, % и д.р.)
  - пароль может повторно использоваться не ранее чем после использования 5-ти отличных от него паролей;
- в случае формирования Администратором ИСПДн персонального пароля пользователя, необходимо:
  - исключить использование одинаковых паролей для учетных записей различных пользователей;

- исключить возможность ознакомления с персональным паролем пользователя любых других работников Учреждения.

3.2. Подсистема регистрации и учета

В подсистеме регистрации и учета реализуются следующие мероприятия по обеспечению безопасности ПДн:

- регистрация входа (выхода) пользователя в систему (из системы) с указанием даты и времени;
- ведение электронных журналов обращений к ПДн, в которых автоматизированными средствами регистрируются запросы пользователей на получение ПДн, а также факты предоставления ПДн по таким запросам. Записи о предоставлении ПДн в электронном журнале обращений должны содержать:
  - идентификатор пользователя;
  - тип события;
  - дата и время события;
  - индикатор успеха или отказа;
  - источник события;
- учет, хранение и уничтожение всех носителей персональных данных (бумажных и машинных), исключающие НСД к таким носителям, в соответствии с разделом 5 настоящего Регламента.

Администратор ИСПДн осуществляет настройку и периодическую проверку электронных журналов обращений во всех прикладных системах ИСПДн с целью выявления попыток и фактов несанкционированного доступа к ПДн. В случае обнаружения попыток или фактов НСД к ПДн, Администратор ИСПДн незамедлительно уведомляет о выявленных фактах Ответственного за обеспечение безопасности ПДн.

3.3. Подсистема обеспечения целостности

В подсистеме обеспечения целостности реализуются механизмы восстановления ПДн, модифицированных или уничтоженных вследствие ошибки пользователя ИСПДн, несанкционированного доступа к ПДн, а также возникновения сбоев или выхода из строя программно-аппаратного обеспечения ИСПДн.

Администратор ИСПДн обеспечивает непрерывное и надежное функционирование в Учреждении подсистемы обеспечения целостности в соответствии со следующими требованиями:

- резервному копированию в Учреждении подлежат все персональные данные, хранящиеся на серверах (в базах данных, личных каталогах пользователей и т.п.), а также на съемных носителях;
- резервное копирование ПДн, хранящихся на съемных носителях, должно осуществляться путем копирования информации на сетевые диски файловых серверов;
- резервное копирование ПДн, хранящихся на серверах, должно осуществляться путем копирования информации на магнитные ленты, RAID-массивы, съемные диски и т.п.;

- периодичность резервного копирования и сроки хранения резервных копий для каждого ресурса определяются Администратором ИСПДн по согласованию с владельцем резервируемого ресурса;
- все создаваемые резервные копии должны содержать отметку о наименовании резервируемого ресурса, а также дате (времени) начала и окончания операций копирования;
- машинные носителей, содержащих резервные копии персональных данных, должны учитываться аналогично любому другому машинному носителю персональных данных;
- должна проводиться периодическая проверка машинных носителей, предназначенных для хранения резервных копий. При выявлении нарушений/сбоев в работе машинного носителя, информация с такого носителя переносится на исправный, а сам носитель уничтожаются;
- восстановление персональных данных из резервной копии производится по заявке (служебной записке) от пользователя. Такая заявка готовится в произвольной форме и должна содержать название базы данных или файла, которые необходимо восстановить, дату и время, по состоянию на которые должны быть восстановлены данные, а также причину, по которой произошла потеря данных;
- Администратор ИСПДн восстанавливает ПДн из резервной копии в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более чем после трех рабочего дней, с момента получения согласованной заявки о восстановлении ПДн.

3.4. Подсистема антивирусной защиты

В подсистеме антивирусной защиты применяются антивирусные средства, предназначенные для защиты рабочих станций и серверов, а также антивирусные средства, предназначенные для использования на сетевых шлюзах (в межсетевых экранах, маршрутизаторах, прокси-серверах) для антивирусного контроля сетевого трафика.

Администратор ИСПДн обеспечивает непрерывное и надежное функционирование в Учреждении подсистемы антивирусной защиты в соответствии со следующими требованиями:

- средства антивирусной защиты должны быть установлены и настроены на всех рабочих станциях и серверах до начала их использования для обработки ПДн;
- модуль средства антивирусной защиты, осуществляющий мониторинг вирусной активности в реальном времени, должен запускаться при загрузке операционной системы в автоматическом режиме вместе с основным модулем средства антивирусной защиты.
- полная антивирусная проверка рабочих станций и серверов должна проводиться:
  - еженедельно в автоматическом режиме;

- после прохождения технического обслуживания или ремонта оборудования сторонними организациями;
- непосредственно после установки (изменения) программного обеспечения;
- в случае обращения работников Учреждения о подозрении или выявлении вредоносного ПО в ИСПДн;

– любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD/DVD – R/RW, USB Flash drive и т.п.) подлежит обязательному антивирусному контролю;
– дистрибутивы ПО должны предварительно, перед установкой, проверяться на отсутствие вредоносных программ;
– обновление антивирусных баз должно производиться в автоматическом режиме не реже одного раза в сутки. В случае невозможности автоматического обновления, обновление баз должно производиться вручную, с той же периодичностью.

При обнаружении вредоносного ПО Администратор ИСПДн выполняет следующие действия:

– уничтожение вредоносного ПО и лечение инфицированных файлов, а также проведение контроля целостности программных компонентов и файлов данных пользователей ИСПДн, в случае успешного лечения;
– в случае если уничтожение вредоносного ПО либо последующее лечение невозможно, программные компоненты и файлы данных пользователей ИСПДн уничтожаются. После уничтожения программных компонентов и файлов данных пользователей ИСПДн их исходная версия восстанавливается из резервной копии;
– после уничтожения вредоносного ПО и лечения/восстановления программных компонентов и файлов данных пользователей ИСПДн, сервер или рабочая станция перезагружается и подвергается повторному антивирусный контролю;
– при обнаружении вредоносного ПО на рабочей станции/сервере, имеющей доступ к локальной сети, проводится проверка всех рабочих станций/серверов, имеющих доступ к данной сети или использующих общие данные или ПО с зараженной рабочей станцией/сервером.

3.5. Подсистема межсетевого экранирования

В подсистеме межсетевого экранирования для разграничения доступа к ресурсам ИСПДн при межсетевом взаимодействии и фильтрации сетевых пакетов применяются программно-аппаратные межсетевые экраны.

Ответственный за обеспечение безопасности ПДн осуществляет:

– эксплуатацию межсетевых экранов в соответствии с эксплуатационной и технической документацией к ним;

– периодическую проверку функционирования межсетевых экранов, предусмотренных эксплуатационной и технической документацией.

3.6. Подсистема анализа защищенности

В подсистеме анализа защищенности реализуются следующие мероприятия по обеспечению безопасности ПДн в ИСПДн:

– контроль настроек программного обеспечения рабочих станций и серверов;
– контроль настроек сетевого оборудования;
– поиск уязвимостей на рабочих станциях, серверах и сетевом оборудовании.

Контроль настроек и поиск уязвимостей в ИСПДн Учреждения осуществляется с помощью специализированных программных средств – сканеров безопасности. Ответственный за обеспечение безопасности ПДн осуществляет:

– периодическое сканирование сети с целью исследования ее топологии, осуществления поиска незащищенных или несанкционированных сетевых подключений, проверки настроек межсетевых экранов и поиска уязвимостей используемого программного обеспечения;
– своевременное обновление базы данных уязвимостей, используемой при сканировании сети;
– подготовку отчетов по результатам сканирования.

По результатам сканирования принимаются меры по устранению выявленных в ИСПДн уязвимостей.

3.7. Подсистема обнаружения вторжений

В подсистеме обнаружения вторжений применяются специализированные средства обнаружения вторжений.

Ответственный за обеспечение безопасности ПДн осуществляет:

– эксплуатацию подсистемы обнаружения вторжений в соответствии с эксплуатационной и технической документацией;
– периодический анализ регистрационных журналов подсистемы обнаружения вторжений, в которых накапливается информация об имевших место сигналах тревоги;
– принятие мер по снижению вероятности вторжений (нарушений безопасности) на основании проведенного анализа регистрационных журналов подсистеме обнаружения вторжений.

3.8. Подсистема защиты от утечек по техническим каналам

В подсистеме защиты от утечек по техническим каналам реализуются мероприятия по исключению возможности просмотра неуполномоченными лицами текстовой и графической информации, содержащей персональные данные, с дисплеев рабочих станций, серверов и демонстрационного оборудования (проекторов, телевизоров и т.п.).

3.9. Подсистема физической защиты

В подсистеме физической защиты, в соответствии с установленным порядком пропускного и внутриобъектового режима, для обеспечения безопасности ПДн применяются следующие меры и средства:

- охрана зданий и помещений от несанкционированного проникновения;
- централизованная система видеонаблюдения;
- системы пожарной сигнализации и пожаротушения;
- автоматизированная система контроля и управления доступом в здания и помещения;
- надежные запираемые замки и металлические двери на входах в серверные и архивные помещения;
- исключение неконтролируемого пребывания неуполномоченных лиц в серверных, архивных и административных помещениях.

4. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

4.1. Предоставление прав доступа к персональным данным

Права доступа к персональным данным в Учреждении предоставляется на постоянной или временной основе.

Оформление работнику прав доступа к ПДн на постоянной основе осуществляется на основании утвержденного в Учреждении Перечня лиц, доступ которых к персональным данным необходим для выполнения ими служебных (трудовых) обязанностей, в следующих случаях:

- зачисление нового работника в штат Учреждения на должность, для выполнения обязанностей которой необходим доступ к ПДн;
- перевод работника Учреждения на должность, для выполнения обязанностей которой необходим доступ к ПДн.

Основанием для оформления работнику временного (разового) права доступа к ПДн является выполнение производственного задания, в рамках которого работнику объективно необходим доступ к ПДн.

Права доступа к персональным данным предоставляются работнику на основании Заявки на предоставление, изменение или прекращение прав доступа к персональным данным (далее - Заявка) в соответствии с порядком, определенном в разделе 4.4 настоящего Регламента.

Работник Учреждения, до предоставления ему прав доступа к ПДн и начала обработки такой информации, должен быть в обязательном порядке ознакомлен с требованиями Положения о порядке обработки и обеспечения безопасности персональных данных и других организационно-распорядительных документов в этой области, а также пройти инструктаж (при необходимости, обучение) по следующим направлениям:

- правила автоматизированной и неавтоматизированной обработки ПДн;
- правила использования прикладных систем и технических средств обработки ПДн;
- правила использования средств антивирусной и парольной защиты, применяемых в ИСПДн Учреждения;
- порядок действий при возникновении внештатных ситуаций;
- ответственность за нарушение правил обработки ПДн.

4.2. Изменение прав доступа к персональным данным

Основанием для изменения прав доступа работника к ПДн является:

- перевод работника на должность, в рамках структурного подразделения или Учреждения, функциональные обязанности которой требуют расширения или сокращения прав доступа к ПДн;
- изменение процесса (процессов) обработки ПДн в Учреждении и/или требований законодательства РФ в области обработки и обеспечения безопасности ПДн, при которых расширяются или сокращаются права доступа к ПДн, закрепленные за определенными должностями работников;

– изменения в организационно-штатной структуре Учреждения;
– служебная необходимость, в рамках которой работнику требуется временное (разовое) расширение прав на обработку ПДн;
– проведение в отношении работника служебного расследования, в рамках которого такому работнику необходимо ограничить права доступа к ПДн.

Изменение прав доступа работника к персональным данным осуществляется на основании Заявки в соответствии с порядком, определенном в разделе 4.4. настоящего Регламента.

В случае изменений в процессе (процессах) обработки персональных данных или в организационно-штатной структуре Учреждения, соответствующие изменения должны быть внесены в Перечень лиц, доступ которых к персональным данным необходим для выполнения ими служебных (трудовых) обязанностей.

4.3. Прекращение прав доступа к персональным данным

Основанием для прекращения прав доступа работника к ПДн является:
– нарушение работником требований организационно-распорядительной документации в области обработки и обеспечения безопасности ПДн;
– перевод работника на другую должность или в другое структурное подразделение, не требующих участия в процессах обработки ПДн;
– достижение заявленных целей, для которых работнику предоставлялся временный (разовый) доступ к ПДн;
– прекращение трудовых отношений с работником.

Прекращение прав доступа работника к персональным данным осуществляется на основании Заявки, направленной непосредственным руководителем работника в соответствии с порядком, определенном в разделе 4.4 настоящего Регламента.

4.4. Порядок рассмотрения и согласования Заявки на предоставление, изменение или прекращение прав доступа к персональным данным

Предоставление, изменение или прекращение прав доступа работника к персональным данным осуществляется Администратором ИСПДн на основании Заявки непосредственного руководителя данного работника.

Заявка подготавливается в виде служебной записки (документальной или электронной) и должна содержать:
– Ф.И.О. работника, которому предоставляется доступ;
– наименование информационной системы, к которой необходимо предоставить доступ;
– основания для предоставления доступа;
– необходимые права доступа в системе (роль).

Срок выполнения Заявки должен быть минимальным, но не превышать 3-х рабочих дней, с момента ее получения Администратором ИСПДн.

Администратор ИСПДн уведомляет направившего Заявку о результате ее исполнения.

5. УЧЕТ, ХРАНЕНИЕ И УНИЧТОЖЕНИЕ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Обращение с бумажными носителями

Учет бумажных (документальных) носителей ПДн в Учреждении осуществляется в соответствии с внутренними нормативными документами, определяющими порядок документооборота.

Бумажные (документальные) носители ПДн должны храниться в охраняемых помещениях и (или) архиве Учреждения, исключающих несанкционированный доступ в них посторонних лиц, в сейфах или запираемых металлических шкафах (ящиках).

Хранение бумажных (документальных) носителей ПДн вместе с документами общего доступа запрещается, за исключением случаев, когда документы общего доступа являются приложениями к бумажным (документальным) носителям ПДн.

Запрещается совместное хранение бумажных (документальных) носителей ПДн, обработка которых осуществляется в различных целях.

Основанием для уничтожения бумажных (документальных) носителей ПДн является:

- достижение целей обработки;
- отзыв согласия субъекта на обработку его ПДн;
- получение соответствующего запроса от субъекта ПДн;
- получение соответствующего указания от уполномоченного органа по защите прав субъектов.

Бумажные (документальные) носители ПДн уничтожаются по мере производственной необходимости.

Уничтожение бумажных (документальных) носителей ПДн производится с помощью специализированных технических средств, исключающих возможность восстановления информации.

5.2. Обращение с машинными носителям

Учету подлежат следующие типы машинных носителей ПДн:

- отчуждаемые носители информации (внешние жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, USB флэш-накопители, карты флэш-памяти, оптические носители (CD, DVD, Blu-ray) и др.);
- неотчуждаемые носители информации (жесткие магнитные диски).

Все машинные носители, используемые для обработки и хранения персональных данных, обязательно регистрируются и учитываются в Журнале учета машинных носителей данных, содержащих ПДн (далее - Журнал). Типовая форма Журнала приведена в Приложении 1 к настоящему Регламенту.

Каждому машинному носителю, содержащему персональные данные, присваивается учетный номер, который наносится на носитель информации.

Неотчуждаемые носители ПДн закрепляются за работниками, ответственными за рабочую станцию (сервер), на которой они установлены.

Отчуждаемые носители ПДн закрепляются за работниками, которым такие носители выдаются для использования в процессах обработки ПДн.

В случае выхода из строя или принятия решения о прекращении использования машинного носителя в процессах обработки ПДн такой носитель сдается Администратору ИСПДн, о чем делается запись о возврате носителя в Журнале.

Ответственность за ведение Журналов несут Администраторы ИСПДн.

Отчуждаемые машинные носители ПДн должны храниться в охраняемых помещениях и (или) архиве Учреждения, исключающих несанкционированный доступ в них посторонних лиц, в сейфах или запираемых металлических шкафах (ящиках).

Хранящиеся на машинных носителях и потерявшие актуальность персональные данные должны своевременно стираться (уничтожаться).

Персональную ответственность за сохранность полученных машинных носителей и предотвращение несанкционированного доступа к записанным на них данным несет работник, за которым закреплены такие носители.

Решение об уничтожении машинного носителя ПДн принимается Администратором ИСПДн, в случае:

- повреждения машинного носителя, исключающего его дальнейшее использование;
- потери практической ценности носителя.

Машинные носители уничтожаются методом физического разрушения, исключающим возможность восстановления информации, о чем делается отметка в Журнале.

6. КОНТРОЛЬНЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В Учреждении не реже одного раза в три года должны проводиться контрольные мероприятия по обеспечению безопасности ПДн в целях:

- проверки выполнения требований организационно-распорядительной документации и действующего законодательства Российской Федерации в области обработки и обеспечения безопасности персональных данных;
- оценки уровня осведомленности работников Учреждения в области обработки и обеспечения безопасности ПДн;
- оценки эффективности применяемых мер и средств защиты.

Контрольные мероприятия проводятся при обязательном участии ответственного за обеспечение безопасности ПДн и Администратора ИСПДн.

По результатам проведения контрольного мероприятия подготавливается отчет, содержащий:

- описание проведенного мероприятия;
- перечень и описание выявленных нарушений;
- выводы по результатам мероприятия и рекомендации по устранению выявленных нарушений

Контрольные мероприятия по обеспечению безопасности СЗПДн могут включать в себя одну или несколько перечисленных ниже проверок:

6.1. Проверки в подсистеме управления доступом

При проведении контрольных мероприятий в подсистеме управления доступом могут выполняться следующие проверки:

- проверка соответствия установленных прав доступа (в прикладных системах, базах данных и т.п.) должностным обязанностям работника;
- проверка соответствия настроек и условий эксплуатации средств защиты информации подсистемы управления доступом требованиям, указанным в эксплуатационной документации таких средств;
- проверка процесса идентификации, аутентификации и авторизации при входе пользователя в систему (обращении к информационным ресурсам ИСПДн);
- проверка механизмов блокирования доступа к средствам обработки и защиты ИСПДн при выполнении устанавливаемого числа неудачных попыток ввода пароля;
- проверка механизма принудительной смены пароля (по истечению его срока действия);
- проверка выполнения требований по стойкости пароля.

6.2. Проверки в подсистеме регистрации и учета

При проведении контрольных мероприятий в подсистеме регистрации и учета могут выполняться следующие проверки:

- проверка системных журналов на наличие зарегистрированных попыток несанкционированного доступа;

– имитация попытки несанкционированного доступа в систему, для проверки работы системы регистрации попытки НСД в системном журнале;
– проверка соответствия настроек и условий эксплуатации средств защиты информации подсистемы регистрации и учета требованиям, указанным в эксплуатационной документации таких средств;
– проверка способов защиты системного журнала регистрации от уничтожения или модификации нарушителем;
– проверка функционирования систем непрерывного мониторинга событий (анализ журналов операционных систем, средств антивирусной защиты, межсетевых экранов и т.п.), которые могут являться причиной реализации угроз безопасности ПДн.

Кроме того, при проведении проверок выполнения порядка учета и хранения носителей персональных данных могут выполняться следующие проверки:

– проверка мест хранения носителей ПДн: сейфов, металлических шкафов (ящиков), а также наличия у них надежных замков;
– проверка выполнения установленного в Учреждении порядка учета и хранения носителей ПДн;
– проверка фактического наличия зарегистрированных машинных носителей ПДн, а также ведения журналов учета таких носителей.

6.3. Проверки в подсистеме обеспечения целостности

При проведении контрольных мероприятий в подсистеме обеспечения целостности могут выполняться следующие проверки:

– проверка механизмов контроля целостности пакетов обновлений средств защиты информации с использованием контрольных сумм;
– проверка соответствия настроек и условий эксплуатации средств обеспечения целостности требованиям, указанным в эксплуатационной документации;
– проверка целостности используемого программного обеспечения, путем вычисления контрольных сумм;
– проверка фактического наличия экземпляров резервных копий;
– имитация выполнения резервного копирования и восстановления данных.

6.4. Проверки в подсистеме антивирусной защиты

При проведении контрольных мероприятий в подсистеме антивирусной защиты могут выполняться следующие проверки:

– проверка рабочих станций и серверов на наличие установленных программных средств антивирусной защиты;
– проверка соответствия настроек и условий эксплуатации средств антивирусной защиты требованиям, указанным в эксплуатационной документации;
– проверка механизма своевременного обновления программных средств антивирусной защиты (в т.ч. баз данных вирусных сигнатур) на всех рабочих станциях и серверах;

– запуск полного сканирования системы антивирусным средством в режиме реального времени;
– проверка антивирусным средством используемых съемных носителей;
– проверка функционирования механизмов автоматической антивирусной проверки подключаемых съемных носителей;
– просмотр журналов и отчетов антивирусного средства на наличие фактов заражения вредоносным ПО.

6.5. Проверки в подсистеме межсетевого экранирования

При проведении контрольных мероприятий в подсистеме межсетевого экранирования могут выполняться следующие проверки:

– проверка соответствия настроек и условий эксплуатации средств межсетевого экранирования требованиям, указанным в эксплуатационной документации;
– имитация попыток проникновения в защищаемый сегмент сети извне, в том числе с применением специального ПО;
– проверка журналов межсетевых экранов на наличие зафиксированных попыток обращения к защищаемым ресурсам.

6.6. Проверки в подсистеме анализа защищенности

При проведении контрольных мероприятий в подсистеме анализа защищенности могут выполняться следующие проверки:

– проверка своевременного обновления ПО, используемого для анализа защищенности, в т.ч. баз данных уязвимостей;
– проверка соответствия настроек и условий эксплуатации сканеров безопасности требованиям, указанным в эксплуатационной документации;
– имитация попыток преодоления СЗПДн, а также проверка системных журналов на фиксирование попыток НСД.

6.7. Проверки в подсистеме обнаружения вторжений

При проведении контрольных мероприятий в подсистеме обнаружения вторжений, выполняются следующие проверки:

– проверка своевременного обновления ПО, используемого для обнаружения вторжений, в т.ч. баз данных уязвимостей;
– проверка соответствия настроек и условий эксплуатации средств обнаружения вторжений требованиям, указанным в эксплуатационной документации;
– имитация попыток вторжения в СЗПДн, а также проверка системных журналов на фиксирование попыток НСД.

6.8. Проверки в подсистеме защиты от утечек по техническим каналам

При проведении контрольных мероприятий в подсистеме защиты от утечек по техническим каналам выполняется проверка размещения дисплеев рабочих станций, серверов и демонстрационного оборудования (проекторов) таким образом, чтобы исключалась возможность просмотра неуполномоченными лицами текстовой и графической информации, содержащей персональные данные.

6.9. Проверки в подсистеме физической защиты

При проведении контрольных мероприятий в подсистеме физической защиты могут выполняться следующие проверки:

- проверка электронных журналов системы контроля и управления доступом на предмет попыток НСД в защищаемые здания и помещения неуполномоченных лиц;
- проверка наличия и условий хранения всех экземпляров ключей (в том числе и электронных пропусков) от защищаемых помещений;
- просмотр всех заявлений об утерянных ключах (в том числе и электронных пропусках) с помощью которых можно получить доступ в защищаемые помещения, а так же проверка принятых мер по фактам их утери;
- проверка надежности замков и дверей, установленных на входах в защищаемые помещения;
- имитация попытки проникновения в защищаемые здания и помещения для проверки срабатывания технических средств охраны и (или) системы контроля и управления доступом.

7. МОДЕРНИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

В целях обеспечения соответствия применяемых в СЗПДн мер и средств защиты актуальным угрозам и требованиям законодательства РФ, в Учреждении проводится модернизация СЗПДн.

Модернизация СЗПДн в обязательном порядке производится в случаях, если:

– в Учреждении была выделена новая ИСПДн;
– изменился состав и/или конфигурация программных и/или технические средств обработки существующих ИСПДн;
– изменились категории обрабатываемых в Учреждении ПДн;
– изменился состав угроз безопасности ПДн в ИСПДн;
– изменился необходимый уровень защищенности ИСПДн.

Ответственность за проведение модернизации СЗПДн Учреждения возложена на Ответственных за обеспечение безопасности ПДн.

Модернизации СЗПДн включает в себя одно или несколько из следующих мероприятий:

– уточнение перечня обрабатываемых ПДн;
– уточнение (проверка и корректировка) состава и структуры ИСПДн;
– формирование (корректировка) модели угроз ПДн;
– классификация ИСПДн;
– выбор (корректировка) применяемых мер и средств защиты ПДн.

7.1. Уточнение перечня обрабатываемых персональных данных

Уточнение перечня обрабатываемых ПДн проводится при возникновении следующих изменений в процессах обработки ПДн:

– изменения категорий субъектов, чьи данные обрабатываются в Учреждении;
– изменения состава обрабатываемых персональных данных;
– изменения правовых оснований обработки ПДн.

Все указанные выше изменения подлежат внесению в Перечень персональных данных, обрабатываемых в Учреждении.

7.2. Уточнение (проверка и корректировка) состава и структуры ИСПДн

При проведении проверки состава и структуры ИСПДн Учреждения оценивается соответствие:

– категорий персональных данных, содержащихся в базах данных (хранилищах) и на отчуждаемых носителях информации утвержденному Перечню персональных данных обрабатываемых.
– конфигурации и топологии ИСПДн в целом и ее отдельных компонентов, а именно перечня серверного оборудования, автоматизированных рабочих мест, общесистемных и прикладных программных средств, задействованных при обработке ПДн, перечня применяемых средств защиты информации, а также сетевой инфраструктуры и сетевого оборудования, утвержденному Перечню информационных систем персональных данных.

7.3. Формирование (корректировка) модели угроз

На основании сведений о составе и структуре ИСПДн, а также об условиях неавтоматизированной обработки ПДн, формируется нормативный документ Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, который содержит в себе следующие сведения:

- перечни характерных для применяемых способов обработки ПДн источников угроз безопасности ПДн, их уязвимостей к угрозам, способов реализации данных уязвимостей, объектов воздействия и последствий реализации вышеуказанных способов;
- анализ и оценку ущерба для субъектов ПДн от реализации угроз безопасности ПДн;
- анализ и оценку актуальности вышеуказанных угроз.

При оценке актуальности угроз используются следующие нормативные документы:

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России 14.02.2008);
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России 15.02.2008).

7.4. Классификация (определение необходимого уровня защищенности) ИСПДн

Классификация ИСПДн в Учреждении проводится в соответствии с документом «Требования к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Постановлением Правительства РФ от 1 ноября 2012 г. №1119).

7.5. Выбор (корректировка) применяемых мер и средств защиты

Выбор (корректировка) применяемых мер и средств защиты производится на основании сформированного перечня актуальных угроз безопасности ПДн, определенных в Модели угроз безопасности ПДн при их обработке в ИСПДн.

В случае если Учреждение привлекает стороннюю организацию для проведения мероприятий по внедрению, настройке, ремонту и сопровождению технических средств защиты информации, такая организация должна обладать лицензией на деятельность по технической защите конфиденциальной информации.

8. ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ

8.1. Права и обязанности Администратора ИСПДн

Администратор ИСПДн обязан:

- обеспечить настройку и бесперебойную эксплуатацию программных и технических средств обработки персональных данных, входящих в состав информационных систем персональных данных Учреждения;
- обеспечить функционирование следующих подсистем защиты СЗПДн, в соответствии с разделом 3 настоящего Регламента:
  - подсистемы управления доступом, регистрации и учета;
  - подсистемы обеспечения целостности (резервного копирования);
  - подсистемы антивирусной защиты;
- настраивать права доступа работников к персональным данным и средствам их обработки в Учреждении;
- хранить дистрибутивы программного обеспечения средств обработки информации ИСПДн;
- обеспечить контроль сторонних организаций (подрядчиков), при привлечении последних для обслуживания, настройки и ремонта средств обработки и защиты информации ИСПДн;
- предоставлять необходимую информацию при проведении проверок регулирующими органами, а также проведении контрольных мероприятий по обеспечению безопасности ПДн;
- предоставлять консультации и оказывать содействие работникам, участвующим в процессах обработки и обеспечения безопасности ПДн, по вопросам использования средств обработки и защиты информации ИСПДн, в рамках своей компетенции.

Администратор ИСПДн имеет право:

- вносить предложения по совершенствованию СЗПДн Учреждения, в том числе организационно-распорядительных документов в области обработки и обеспечения безопасности ПДн;
- запрашивать у работников, участвующих в процессах обработки и обеспечения безопасности ПДн, информацию и документы, необходимые для выполнения функциональных обязанностей.

8.2. Права и обязанности Ответственного за обеспечение безопасности ПДн

Ответственный за обеспечение безопасности ПДн обязан:

- организовать построение и эксплуатацию системы защиты персональных данных Учреждения и, при необходимости, организовать модернизацию СЗПДн в соответствии с разделом 7 настоящего Регламента;
- обеспечить поддержание в актуальном состоянии организационно-распорядительных документов учреждения по обработке и обеспечению безопасности ПДн;
- обеспечить функционирование следующих подсистем защиты СЗПДн, в соответствии с разделом 3 настоящего Регламента:

- подсистемы межсетевого экранирования;
- подсистемы обнаружения и предотвращения вторжений;
- подсистемы защиты от утечек по техническим каналам;
- подсистемы анализа защищенности (сетевых сканеров).

– осуществлять проведение контрольных мероприятий по обеспечению безопасности персональных данных в соответствии с разделом 6 настоящего Регламента;
– хранить дистрибутивы программного обеспечения средств защиты информации ИСПДн, а также эксплуатационную документацию и сертификаты средств защиты информации;
– вести поэкземплярный учет применяемых средств защиты информации;
– организовать учет, хранение и уничтожение машинных носителей персональных данных;
– организовать проведение инструктажей и обучения работников Учреждения, по вопросам обработки и обеспечения безопасности персональных данных;
– осуществлять взаимодействие с регулирующими органами по вопросам обработки и обеспечения безопасности ПДн, в том числе координировать действий работников Учреждения при проведении проверок регулирующими органами, а также при обработке запросов указанных органов;
– предоставлять консультации и оказывать содействие работникам Учреждения по вопросам обеспечения безопасности персональных данных, в рамках своей компетенции;

Ответственный за обеспечение безопасности ПДн имеет право:

– вносить предложения по совершенствованию СЗПДн Учреждения, в том числе организационно-распорядительных документов в области обработки и обеспечения безопасности ПДн;
– запрашивать у работников, участвующих в процессах обработки и обеспечения безопасности ПДн, информацию и документы, необходимые для выполнения функциональных обязанностей.

8.3. Ответственность

Администраторы ИСПДн и Ответственные за обеспечение безопасности ПДн несут дисциплинарную ответственность за невыполнение и/или ненадлежащее выполнение требований настоящего Регламента, а также других организационно-распорядительных документов Учреждения, в области обработки и обеспечения безопасности ПДн.

Прекращение доступа к персональным данным и/или увольнение не освобождает работника Учреждения от принятых обязательств по неразглашению персональных данных, ставших доступными при выполнении должностных обязанностей.

Незаконное распространение, раскрытие третьим лицам или использование в личных целях персональных данных влечет за собой ответственность, предусмотренную законодательством Российской Федерации.

ПРИЛОЖЕНИЕ 1

ТИПОВАЯ ФОРМА ЖУРНАЛА УЧЕТА МАШИННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

ЖУРНАЛ

учёта машинных носителей персональных данных

№ п/п	Ф.И.О. работника	Дата получения и подпись работника	Номер машинного носителя	Тип носителя	Ф.И.О. Администратора ИСПДн	Дата возврата и подпись работника	Отметка об уничтожении	Дата уничтожения и подпись Администратора
1.								
2.								
3.								
4.								