МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ
«СВЕРДЛОВСКИЙ ОБЛАСТНОЙ ЦЕНТР ПРОФИЛАКТИКИ И БОРЬБЫ СО СПИД»
(ГБУЗ СО ОЦ СПИД)

ПРИКАЗ

Екатеринбург

28.10.2015 года **№45-в**

Об утверждении Положения об организации и проведении работ по обеспечению безопасности персональных данных обрабатываемых в информационных системах персональных данных и/или без использования средств автоматизации

Во исполнение Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, на основании Федерального закона от 21.11.2011 № 323 ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

ПРИКАЗЫВАЮ:

1. Утвердить положение об организации и проведении работ в ГБУЗ СО «ОЦ СПИД» по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Приложение № 1).
2. Заместителю главного врача по хозяйственным вопросам Ершову В.М. в срок до 15.12.2015 организовать разработку и утверждение типовых форм журналов:
   - учета установленных средств защиты информации;
   - журнала учета машинных носителей;
   - журнала учета хранилищ;
   - журнала периодического тестирования средств защиты;
   - журнала учета нештатных ситуаций информационных систем персональных данных (далее-ИСПДн), выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн;
   - журнала учета пользователей, допущенных к информационным системам персональных данных;
   - журнала проверок электронных журналов;
   - журнала учета обращений субъектов персональных данных о выполнении их законных прав.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач А.С. Подымова

Приложение №1,
утверждено приказом
№45-в от 28.10.2015

ПОЛОЖЕНИЕ
по организации и порядку проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Государственного бюджетного учреждения Свердловской области «Свердловский областной центр профилактики и борьбы со СПИД»

1. Термины и определения

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

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;

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;

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

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

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических

средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

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;

Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

Угроза или опасность утраты персональных данных - единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

2. Общие положения

2. Настоящее положение разработано на основе Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781.

2. Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия. Для защиты ПДн создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Мероприятия по обеспечению безопасности ПДн формулируются в зависимости от класса ИСПДн, определяемого с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, общества и государства.

2. Для обеспечения безопасности ПДн при их обработке в ИСПДн осуществляется защита информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в ИСПДн. Для защиты персональных данных необходимо соблюдать ряд мер:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют работы с персональными данными;
- строгое избирательное и обоснованное распределение документов и информации между работниками; рациональное размещение рабочих мест,

при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудниками предприятия требований нормативно-методических документов по защите информации;
- наличие необходимых условий в помещениях для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещения, в которых функционируют ИСПДн;
- организация порядка уничтожения информации;
- своевременное выявление нарушений требований разрешительной системы доступа к ПДн; обучение сотрудников, воспитательная и разъяснительная работа по вопросам информационной безопасности;
- определение и регламентация состава сотрудников, имеющих право доступа к информационным ресурсам ИСПДн.

3. Основные мероприятия по организации обеспечения безопасности персональных данных.

3.1 Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн.

3.2 Обязанности по реализации необходимых организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними, возлагаются на Государственное учреждение здравоохранения Свердловской области «Свердловский областной центр профилактики и борьбы со СПИД» как оператора, осуществляющего обработку персональных данных.

3.3 Ответственным за обеспечение безопасности ПДн при их обработке в информационных системах персональных данных Государственное учреждение здравоохранения Свердловской области «Свердловский областной центр профилактики и борьбы со СПИД»назначен заместителя главного врача по хозяйственным вопросам. Функции по разработке и осуществлению мероприятий по организации и обеспечению безопасности ПДн при их обработке в информационных системах персональных данных возложены на заместителя главного врача по хозяйственным вопросам.

3.4 Технические и программные средства, используемые для обработки ПДн в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

3.5 Обработка персональных данных должна осуществляться на основе принципов: законности целей и способов обработки персональных данных и добросовестности; соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;

3.6 соответствия объема и характера обрабатываемых персональных данных,

способов обработки целям обработки персональных данных;
3.7 достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
3.8 недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.
3.9 Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы (подсистемы) защиты персональных данных (СЗПДн). Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации, а также используемые в информационной системе информационные технологии.
3.10 Сотрудники предприятия, ответственные за хранение персональных данных, а также сотрудники предприятия, владеющие персональными данными в силу своих должностных обязанностей, подписывают Обязательство о конфиденциальности (Приложение 1).
3.11 Помещения, в которых хранятся и обрабатываются персональные данные, должны быть оборудованы надежными замками и сигнализацией на вскрытие помещений, в рабочее время данные помещения при отсутствии в них работников должны быть закрыты, проведение уборки помещений должно производиться в присутствии работников подразделений, ответственных за данные помещения.

4. Обязанности должностных лиц, эксплуатирующих ИСПДн, в части обеспечения безопасности персональных данных при их обработке в ИСПДн

При обработке персональных данных предприятие, выполняя функции оператора ПДн, обязано соблюдать следующие требования:

- обработка персональных данных осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации;
- обработка персональных данных пациентов предприятия осуществляется в целях оказания медицинской помощи;
- персональные данные следует получать лично у субъекта ПДн. в случае возникновения необходимости получения персональных данных субъекта у третьей стороны следует известить об этом объект ПДн заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных;
- запрещается получать, обрабатывать и вносить в ИСПДн не установленные Федеральными законами "О персональных данных" персональные данные о политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах;
- при принятии решений, затрагивающих интересы субъекта ПДн, запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;
- защита персональных данных от неправомерного их использования

способов обработки целям обработки персональных данных;
3.7 достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
3.8 недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.
3.9 Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы (подсистемы) защиты персональных данных (СЗПДн). Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации, а также используемые в информационной системе информационные технологии.
3.10 Сотрудники предприятия, ответственные за хранение персональных данных, а также сотрудники предприятия, владеющие персональными данными в силу своих должностных обязанностей, подписывают Обязательство о конфиденциальности (Приложение 1).
3.11 Помещения, в которых хранятся и обрабатываются персональные данные, должны быть оборудованы надежными замками и сигнализацией на вскрытие помещений, в рабочее время данные помещения при отсутствии в них работников должны быть закрыты, проведение уборки помещений должно производиться в присутствии работников подразделений, ответственных за данные помещения.

4. Обязанности должностных лиц, эксплуатирующих ИСПДн, в части обеспечения безопасности персональных данных при их обработке в ИСПДн

При обработке персональных данных предприятие, выполняя функции оператора ПДн, обязано соблюдать следующие требования:

- обработка персональных данных осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации;
- обработка персональных данных пациентов предприятия осуществляется в целях оказания медицинской помощи;
- персональные данные следует получать лично у субъекта ПДн. в случае возникновения необходимости получения персональных данных субъекта у третьей стороны следует известить об этом объект ПДн заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных;
- запрещается получать, обрабатывать и вносить в ИСПДн не установленные Федеральными законами "О персональных данных" персональные данные о политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах;
- при принятии решений, затрагивающих интересы субъекта ПДн, запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;
- защита персональных данных от неправомерного их использования

или утраты обеспечивается за счет средств оператора в порядке, установленном Федеральными законом "О персональных данных", Трудовым кодексом Российской Федерации и иными нормативными правовыми актами Российской Федерации;

- передача персональных данных субъекта ПДн третьей стороне не допускается без письменного согласия субъекта, за исключением случаев, установленных федеральными законами Российской Федерации;
- обеспечивается конфиденциальность персональных данных, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;
- в случае выявления недостоверных персональных данных или неправомерных действий с ними сотрудников Государственное учреждение здравоохранения Свердловской области «Свердловский областной центр профилактикb и борьбы со СПИД», осуществляющих обработку ПДн, при обращении или по запросу субъекта персональных данных, или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных, Государственное учреждение здравоохранения Свердловской области «Свердловский областной центр профилактики и борьбы со СПИД», как оператор ПДн, обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту, с момента такого обращения или получения такого запроса на период проверки;
- в случае подтверждения факта недостоверности персональных данных субъекта персональных данных сотрудники Государственное учреждение здравоохранения Свердловской области «Свердловский областной центр профилактики и борьбы со СПИД», осуществляющие обработку ПДн, на основании документов, представленных субъектом персональных данных, или его законным представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязаны уточнить персональные данные и снять их блокирование;
- в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, допущенные нарушения должны быть устранены, в случае невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, персональные данные должны быть уничтожены. Об устранении допущенных нарушений или об уничтожении персональных данных Государственное учреждение здравоохранения Свердловской области «Свердловский областной центр профилактики и борьбы со СПИД» как оператор ПДн, обязан уведомить субъекта ПДн, или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган;
- хранение персональных данных должно осуществляться в форме, позволяющей определить субъект персональных данных, не дольше,

чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

5. Порядок предоставления информации, содержащей персональные данные

5.1 Предоставление и пользование информацией, содержащей персональные данные субъекта, осуществляется на основании письменного разрешения техника отдела компьютерного обеспечения. Передача и предоставление ПДн законным пользователям должна осуществляться способом, не допускающим возможность несанкционированного доступа к ним посторонних лиц.

5.2 Передача информации, содержащей персональные данные субъекта ПДн, другим учреждениям и организациям, осуществляется только при наличии правомерных письменных запросов и с письменного разрешения техника отдела компьютерного обеспечения в размере, который позволяет не разглашать излишний объем персональных сведений.

5.3 При передаче персональных данных субъекта ПДн оператор должен соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия субъекта,
- за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья субъекта ПДн, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными субъектов ПДн в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
- передавать персональные данные субъекта ПДн представителю этого субъекта в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

5.4 При обращении с запросом о персональных данных пациента Государственное учреждение здравоохранения Свердловской области «Свердловский областной центр профилактики и борьбы со СПИД» лица, не уполномоченного федеральным законом на получении персональных данных, либо при отсутствии письменного согласия пациента на предоставление его персональных данных учреждение обязано отказать в предоставлении персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.

6. Порядок приостановки предоставления ПДн в случае обнаружения нарушения порядка их предоставления

6.1. В случае обнаружения нарушений порядка предоставления ПДн ответственным за обеспечение безопасности ПДн выносится предписание, по которому приостанавливается обработка ПДн до выяснения и устранения причин нарушений.

6.2. Регистрация и расследование фактов нарушения порядка предоставления ПДн проводится в соответствии с разделом 14 данного Положения.

7. Порядок организации ведения и периодической проверки электронного журнала обращений пользователей информационной системы к ПДн

7.1. Запросы пользователей информационных систем ПДн предприятия на получение персональных данных, включая лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений.

7.2. Содержание электронного журнала обращений периодически, но не реже одного раза в месяц, проверяется администратором информационной безопасности.

8. Правила парольной защиты

8.1. В системе управления доступом должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в операционную систему ИСПДн. Возможно применение двух вариантов авторизации:

- по паролю условно-постоянного действия, длиной не менее семи буквенно-цифровых символов;
- с использованием электронного идентификатора, который служит для авторизации пользователя на компьютерах с установленным СЗИ.

8.2. Персональные пароли должны выбираться следующих требований:

в составе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы;

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 (2,3..,7,8) позициях;
- личный пароль пользователь не имеет права сообщать никому;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abed и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе.

8.3. При вводе пароля пользователю необходимо исключить возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерам и т.п.).

8.4. Порядок смены личных паролей:

- Смена паролей должна проводиться регулярно, не реже 1 раза в 3 месяца.
- В случае прекращения полномочий пользователя (увольнение, либо переход на другую работу) производится немедленное удаление его идентификационных данных.
- Срочная (внеплановая) полная смена паролей должна производится в случае прекращения полномочий (увольнение или переход на другую работу) администраторов информационной системы и других сотрудников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.
- Администратор ведет "Журнал принудительной смены личных паролей", в котором отмечает причины внеплановой смены паролей пользователей.
- Временный пароль, заданный администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

8.5. Хранение пароля.

- Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях
- информации, в том числе на предметах.
- Запрещается оставлять без присмотра рабочее место с незаблокированным монитором;
- Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.
- Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у администратора или руководителя подразделения.

8.6. Ответственность при организации парольной защиты.

- Владельцы паролей должны быть ознакомлены под подпись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.
- Ответственность за организацию парольной защиты в организации возлагается на администраторов.
- Периодический контроль за соблюдением требований парольной защиты возлагается на техника отдела компьютерного обеспечения.

8.7. В том случае, если на ПК пользователя установлена СЗИ, оснащенная электронными идентификаторами, то пароль записывается в персональный идентификатор пользователя, в идентификатор записывается имя пользователя и его пароль. Пользователь не знает и не должен знать свой пароль. Пользователь осуществляет вход в систему с использованием идентификатора. Идентификатор также может хранить в своей памяти и криптоключ пользователя. Запись пароля в идентификатор производится администратором:

- администратор производит генерацию новых паролей к учетным записям и выдачу ключей пользователям;
- администратор по согласованию с администратором информационной безопасности осуществляет запись криптографического ключа в идентификатор пользователя.

8.8. Устанавливаются следующие парольные политики:

Политика	Параметр безопасности
Макс. Срок действия пароля	3 месяца
Мин. длина пароля	7 символов
Мин. Срок действия пароля	0 дней
Пароль должен отвечать требованиям сложности	Включен
Требовать неповторяемости паролей	1 хранимых паролей
Хранить пароли всех пользователей в домене, используя обратимое шифрование	Отключен

8.9. Пользователь, получивший электронный идентификатор для доступа к ИСПДн, обязан:

- обязательно использовать идентификатор для входа в систему;
- не передавать идентификатор другим пользователям;
- хранить идентификатор в «надежном месте» - например на связке ключей, в сейфе, в шкафу; не хранить идентификатор рядом со считывателем, на столе\системном блоке, в первом ящике стола, на видном месте;
- бережно хранить идентификатор, избегать падений идентификатора, воздействий сильных электромагнитных полей, попадания жидкости на идентификатор;
- если идентификатор содержит криптоключ, быть аккуратным при шифровании и расшифровке папок и файлов;
- в случае утери идентификатора немедленно сообщить об этом одному из администраторов информационной безопасности, а в случае их отсутствия - администраторам.

8.10 Порядок хранения и смены личных паролей:

- смена пароля проводится один раз в год, так как, пароль пользователя, хранящийся в памяти идентификатора, представляет собой набор случайных символов, например 62oqi51v4e0p, такой пароль очень сложно подобрать, пользователь не может изменить свой пароль т.к. не знает его; смену пароля производит администратор; список паролей пользователей хранится у администраторов;
- изменение пароля производится локально, пользователь должен принести ключ администратору для смены пароля, администратор изменяет пароль пользователя и записывает новый пароль в идентификатор;
- администратор, в случае необходимости (фиксация нарушений, увольнение сотрудника и т.п.), может принудительно изменить пароль пользователя. Тогда пароль пользователя в системе не совпадет с паролем в идентификаторе и пользователь не сможет войти в систему.

9. Правила антивирусной защиты

9.1 Антивирусное и другое программное обеспечение, используемое для защиты от вредоносных программ, должно быть лицензированным и приобретенным на законном основании.

9.2 Обязательным условием полноценного функционирования указанного ПО является заключение договоров на его обновление и сопровождение

9.3 Пользователям ИСПДн запрещено самостоятельное копирование и установка ПО любого назначения. Копирование или установка какого-либо ПО должны производиться исключительно администратором ИБ. Для правильной работы необходимо:

9.4 Настроить внутренний планировщик антивирусного ПО на автоматическую загрузку обновлений. При невозможности автоматической загрузки ежедневно производить загрузку обновлений антивирусного ПО и производить обновления.

9.5 Настройку антивирусного ПО выполнить в соответствии с утвержденным «Регламентом настройки политик безопасности при эксплуатации СЗИ».

9.6 Не запускать файлы, полученные от ненадежного источника, прежде чем они не будут проверены антивирусной программой с последними обновлениями.

9.7 В обязательном порядке проверять антивирусным ПО все внешние накопители информации (оптические диски, флэш-накопители, карты памяти, сменные и внешние жесткие диски).

10. Правила обновления общесистемного и прикладного программного обеспечения ИСПДн

10.1 Для функционирующих ИСПДн доработка (модернизация, обновления ПО) СЗПДн должна проводиться в случае, если:

- изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);
- изменился состав угроз безопасности ПДн в ИСПДн; изменился класс ИСПДн.

10.2 Обновления общесистемного и прикладного программного обеспечения ИСПДн осуществляются под контролем техника отдела компьютерного обеспечения при необходимости - специализированных организаций.

11. Требования к помещениям, в которых располагаются ИСПДн

11.1 ПДн, обрабатываемые в ИСПДн, являются информационными данными, защищаемыми в соответствии с требованиями, установленными законодательством Российской Федерации.

11.2 В соответствии с требованиями ИБ, архивы ПДн и ИСПДн (как на электронных, бумажных, так и на иных носителях), оборудование, доступ к которому должен быть ограничен в силу его важности для технологического цикла предприятия (помещения серверных, АТС, АРМов и т.п.), а также обработка ПДн в ИСПДн должны производиться в помещениях, относящихся к категории «помещения ограниченного доступа».

11.3 Помещения ограниченного доступа должны располагаться в контролируемой зоне.

11.4 Пребывание посторонних лиц в помещениях разрешено только в сопровождении сотрудников, работающих в указанных помещениях, и только с разрешения руководства вышеупомянутых сотрудников.

11.5 Допуск в помещения ограниченного доступа вспомогательного и обслуживающего персонала (уборщиц, электромонтеров, сантехников и т.д.) производится только в случае служебной необходимости.

11.6 В случае, когда помещения ограниченного доступа располагаются на первых и последних этажах здания, их окна должны быть оснащены сигнализацией.
11.7 Двери помещений ограниченного доступа не должны отличаться от дверей других помещений и не должны иметь обозначающих и предупреждающих надписей и табличек.
11.8 Внутренняя планировка и расположение рабочих мест в помещениях ограниченного доступа должны обеспечивать исполнителям работ недоступность и сохранность доверенных им ПДн.
11.9 На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, в которых предусматривается порядок вызова администрации, должностных лиц, вскрытие помещений ограниченного доступа, очередность и порядок спасения документов, материалов и изделий, содержащих ПДн, а также порядок дальнейшего их хранения.
11.10 Помещения ограниченного доступа, предназначенные для размещения архивов ПДн, предназначенные для размещения АРМ выработки ключей шифрования и ЭЦП, предназначенные для размещения оборудования, доступ к которому должен быть ограничен, должны отвечать следующим требованиям:

- помещение должно располагаться в контролируемой зоне;
- двери помещения должны иметь надежные запоры, приспособления для опечатывания, либо должны быть оснащены контроллерами, включенными в систему контроля ограничения доступа;
- желательно наличие видеокамеры включенной в систему видеозаписи, контролирующей вход в помещение;
- должны быть задействованы все меры, исключающие неконтролируемое пребывание в помещении любых лиц, включая сотрудников организации, не допущенных к работе с ПДн;
- помещение должно быть оборудовано датчиками пожарной и охранной сигнализации, желательно имеющими отдельные (не связанные с другими помещениями) шлейфы сигнализации, включенные в пульты охранно-пожарной сигнализации;
- помещение должно быть оборудовано средствами пожаротушения, желательно наличие автономной автоматической системы пожаротушения;
- помещение должно быть оборудовано необходимым количеством стеллажей и/или шкафов для хранения архивных носителей;
- микроклимат (температурно-влажностный режим) помещения должен отвечать требованиям по сохранности архивных носителей, а условия хранения должны исключать возможность их повреждения (коробления, пересыхания, изгиба и вредного воздействия пыли, магнитных и электрических полей или ультрафиолета);
- от двери помещения должны быть резервные ключи;
- помещение, предназначенное для хранения резервных копий, не должно совмещаться с помещением, в котором размещается оборудование, создающее и (или) использующее указанные резервные копии.
- размещение в помещении оборудования и вспомогательных технических средств должно отвечать санитарно-гигиеническим нормам, а также требованиям техники безопасности и пожарной

безопасности.

11.11 Работник, осуществляющий хранение архивов и/или резервных копий ИСПДн, должен иметь печать для опечатывания дверей и сейфа или металлического хранилища.

11.12 Выполнение требований по обеспечению ИБ на рабочих местах осуществляется работниками, работающими в помещениях ограниченного доступа.

11.13 Ответственность за невыполнение требований по ИБ для помещений ограниченного доступа несут руководители структурных подразделений, работники которых работают в этих помещениях.

12. Порядок проведения служебной проверки при нарушениях режима безопасности при обработке ПДн в ИСПДн

12.1 Служебная проверка при нарушениях режима безопасности при обработке ПДн в ИСПДн (далее - служебная проверка) проводится для определения уровня защищенности ИСПДн и мер по возможному предотвращению инцидентов ИБ.

12.2 Служебная проверка назначается по нарушениям 1 и 2 категорий по каждому отдельному факту нарушения.

12.3 Основаниями для назначения служебной проверки являются устное заявление, докладная или служебная записка работника Государственное учреждение здравоохранения Свердловской области «Свердловский областной центр профилактики и борьбы со СПИД», а также выявление факта одного или нескольких нарушений.

12.4 Состав комиссии, а также сроки проведения служебного расследования назначаются распоряжением руководителя, ответственного за обеспечение безопасности ПДн, по каждому отдельному факту нарушения или по факту группы нарушений.

12.5 В состав комиссии в обязательном порядке входят:

- председатель комиссии - Ершов Виталий Михайлович - заместитель врача по хозяйственным вопросам.

Члены комиссии:

- Гусев Антон Георгиевич - начальник отдела компьютерного обеспечения;
- Нохрин Александр Сергеевич - техник отдела компьютерного обеспечения.

12.6 В случае необходимости Председатель комиссии может привлекать к работе:

- непосредственного начальника нарушителя;
- экспертов из других подразделений;
- специалистов организаций-лицензиатов.

12.7 Члены комиссии имеют право:

- требовать документального подтверждения факта нарушений информационной безопасности ИСПДн; устанавливать причины допущенных нарушений любым из способов, не противоречащих законодательству РФ;
- брать письменные объяснения по поводу выявленных нарушений у любого сотрудника Государственное учреждение здравоохранения Свердловской области «Свердловский областной центр профилактики

и борьбы со СПИД».

12.8По результатам работы комиссии оформляется акт о результатах служебной проверки, в котором указывается:

- документальное подтверждение факта нарушений ИБ ИСПДн;
- установленные причины выявленных нарушений в ИБ ИСПДн;
- предложения по устранению причин выявленных инцидентов ИБ в ИСПДн; предложения по дополнению Перечня нарушений ИБ.

12.9Акт о результатах служебной проверки подписывается членами комиссии и направляется руководителю, назначившему служебную проверку.

13 Перечень нарушений ИБ ИСПДн

13.1 К нарушениям 1 категории относятся события, повлекшие за собой разглашение (утечку) защищаемых ПДн и/или утрату содержащих их отчуждаемых носителей, уничтожение (искажение) баз данных ИСПДн, выведение из строя технических и программных средств, а именно:

- несанкционированная переконфигурация параметров ИСПДн;
- утрата или кража резервной копии базы данных ИСПДн;
- необоснованная передача базы данных ИСПДн; организация утечки ПДн ИСПДн по техническим каналам; умышленное нарушение работоспособности ИСПДн;
- НСД к ПДн ИСПДн;
- несанкционированное внесение изменений в базу данных ИСПДн;
- умышленное заражение компьютеров и серверов ИСПДн вирусами;
- проведение работ с ИСПДн, повлекшее за собой необратимую потерю данных; другие действия, подпадающие под действия статей 272, 273, 274 УК РФ.

13.2 К нарушениям 2 категории относятся события, в результате которых возникают предпосылки к разглашению (утечке) защищаемых ПДн, утрате содержащих их отчуждаемых носителей, уничтожению (искажению) баз данных ИСПДн, выведению из строя технических и программных средств, а именно:

- подбор административного пароля (успешный);
- ошибка при входе в ИСПДн (набор не назначенного пароля, более трех раз подряд, периодически);
- несанкционированное (неоднократное) оставление включенного ПК;
- утрата учтенного отчуждаемого съемного носителя;
- попытка входа под чужим именем, паролем, многократная неудачная;
- попытка входа под чужим именем, паролем, удачная;
- несанкционированная очистка журналов аудита; несанкционированное копирование ПДн на внешние носители; несанкционированная установка (удаление) ПО на ПК ИСПДн;
- несанкционированное изменение конфигурации ПО ПК ИСПДн;
- попытка получения прав администратора на локальном ПК (увеличения собственных прав, получение прав на отладку программ), удачная и неудачная;
- попытка получения прав администратора в домене или на удаленной машине, удачная и неудачная; неумышленное заражение локального или сетевого ПК компьютерными вирусами, несанкционированное использование сканирующего ПО;

- несанкционированное использование анализаторов протоколов (снифферов);
- несанкционированный просмотр, вывод на печать ПДн.

13.3. К нарушениям 3 категории относятся события, не несущие признаков нарушений 1 и 2 категорий, а именно:

- ошибка при входе в ИСПДн (набор неправильного пароля, сетевого имени более трех раз подряд);
- попытка неудачного доступа к ПДн ИСПДн (периодическая);
- перевод времени на ПК;
- работа на ПК в неразрешенное время;
- перезагрузка компьютера при сбоях в работе ПК (однократная), в т.ч. аварийная перезагрузка, путем нажатия кнопки RESET;
- нецелевое использование корпоративных ресурсов (печать, Internet, mail, и др.).

14 Порядок контроля за соблюдением условий использования средств защиты информации

14.1 Контроль за соблюдением условий использования СЗИ осуществляет техник отдела компьютерного обеспечения в соответствии с выработанным регламентом.

14.2 Контроль осуществляется посредством плановых проверок, мониторинга, тестирования СЗИ ИСПДн.

14.3 По результатам проверок составляется акт, при выявлении замечаний - предписание на устранение выявленных замечаний.

15. Государственный контроль и надзор за эксплуатацией аттестованных ИСПДн

15.1. Государственный контроль и надзор за проведением аттестации ИСПДн по требованиям безопасности информации, а также за соблюдением правил эксплуатации аттестованных ИСПДн и эффективностью принятых мер защиты некриптографическими методами проводятся ФСТЭК России и ее территориальными органами.

15.2. Объем, содержание и порядок государственного контроля и надзора устанавливаются нормативными и методическими документами по обеспечению безопасности ПДн при их обработке в ИСПДн. Контрольные мероприятия проводятся в соответствии с утвержденными планами работ.

15.3. Государственный контроль и надзор за соблюдением правил аттестации включает проверку правильности и полноты проводимых мероприятий по аттестации ИСПДн, проверку правильности оформления отчетных документов и протоколов аттестационных испытаний, проверку своевременности внесения изменений в организационно-распорядительные документы по обеспечению безопасности ПДн, а также контроль за эксплуатацией аттестованных ИСПДн.

15.4. При выявлении нарушения правил эксплуатации аттестованных по требованиям безопасности информации ИСПДн, нарушения технологии обработки ПДн и требований по обеспечению безопасности ПДн Управлением ФСТЭК России по Уральскому федеральному округу может быть приостановлено действие аттестата.

15.5. В случае, когда в результате оперативного принятия организационно-технических мер защиты не может быть восстановлен требуемый уровень безопасности ПДн, может быть принято решение об аннулировании действия

аттестата соответствия.

15.6. При выявлении в ходе контроля и надзора грубых нарушения требований нормативных и методических документов по обеспечению безопасности ПДн, допущенных организацией-лицензиатом, оператор вправе требовать от организации-лицензиата безвозмездного проведения повторной аттестации в соответствии со статьями 723, 783 Гражданского кодекса Российской Федерации.

16. Порядок взаимодействия с вышестоящими службами и федеральными органами

16.1. Уведомление об обработке персональных данных направляется в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор).

16.2. Получение Выписки регламентируется Приказом Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия от 28.03.2008 г. №154 «Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных».

16.3. Операторы, включенные в Реестр, вправе получить выписку из Реестра по письменному обращению в Службу в срок не позднее тридцати дней.

17. Общедоступные источники персональных данных сотрудников предприятия

17.1 В целях информационного обеспечения на предприятии могут создаваться общедоступные источники персональных данных сотрудников (далее - Справочники), в которые с письменного согласия субъекта персональных данных включаются его фамилия, имя, отчество, сведения о занимаемой им должности, номер служебного телефона, иные персональные данные, предоставленные субъектом персональных данных.

17.2 Формирование, ведение и иные действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, содержащихся в Справочниках, а также получение письменного согласия субъекта персональных данных осуществляются подразделениями предприятия, ответственными за ведение каждого Справочника.

18. Ответственность за нарушение требований, регулирующих получение, обработку и хранение персональных данных сотрудника

19.1 Лица, виновные в нарушении требований, регулирующих получение, обработку и хранении персональных данных сотрудника несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

19.2 Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы:

- руководитель, разрешающий доступ сотрудника к персональным данным несет персональную ответственность за данное разрешение;
- каждый сотрудник несет единоличную ответственность за сохранность носителей персональных данных и соблюдение конфиденциальности информации;
- сотрудник Государственное учреждение здравоохранения

Свердловской области «Свердловский областной центр профилактики и борьбы со СПИД», предоставивший работодателю подложные документы или заведомо ложные сведения о себе, либо своевременно не сообщивший об изменениях персональных данных, несет дисциплинарную ответственность, вплоть до увольнения.

- Лица, виновные в нарушении условий использования средств защиты информации или нарушении режима защиты персональных данных, несут ответственность в соответствии с законодательством Российской Федерации.