Приложение № 3 к приказу № 11 от 11.01.2016 г.

ПОЛОЖЕНИЕ
ОБ ОРГАНИЗАЦИИ И ПОРЯДКЕ ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ
государственного бюджетного учреждения здравоохранения Свердловской области «Городская поликлиника № 3 город Нижний Тагил»

Термины и определения

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

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

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.

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

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 обработки персональных данных (за исключением случаев, если обработка необходима для уточнения 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.

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

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических 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 на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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.

1. Общие положения

1.1. Настоящее положение разработано на основе Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», 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.

1.2. 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.

1.3.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.

1.4. 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.

2. Основные мероприятия по организации обеспечения безопасности персональных данных

2.1.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.

2.2.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 ГБУЗ СО «ГП № 3 г. Нижний Тагил» как оператора, осуществляющего обработку персональных данных.

2.3.Ответственным за обеспечение безопасности ПДн при их обработке в информационных системах персональных данных ГБУЗ СО «ГП № 3 г. Нижний Тагил» назначен техник В.А.Ветлицин. Функции по разработке и осуществлению мероприятий по организации и обеспечению безопасности ПДн при их обработке

в информационных системах персональных данных возложены на техника В.А.Ветлицина.

2.4.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.

2.5.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;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

2.6.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.

2.7.Сотрудники Оператора, ответственные за хранение персональных данных, а также сотрудники Оператора, владеющие персональными данными в силу своих должностных обязанностей, подписывают Обязательство о неразглашении.

2.8.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.

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

4.1Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или

случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

4.2Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

4.3Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

4.4 Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 3 Федерального закона N 261-ФЗ требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

4.5 Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

4.6 Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 Федерального закона N 261-ФЗ, операторы вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности операторов, с учетом содержания персональных данных, характера и способов их обработки.

4.7 Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

4.9 Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не

являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

4.10 Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

4.11 Под угрозами безопасности персональных данных понимается 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. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

5.Порядок предоставления информации, содержащей персональные данные

5.1 При сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона N 261-ФЗ "О внесении изменений в Федеральный закон "О персональных данных"". Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 Федерального закона N 261-ФЗ статьи 14, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные настоящим Федеральным законом права субъекта персональных данных;

5) источник получения персональных данных.

Передача информации, содержащей персональные данные субъекта ПДн, другим учреждениям и организациям, осуществляется в порядке, установленном Оператором.

5.2 Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, в случаях, если:

1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

5) предоставление субъекту персональных данных сведений, нарушает права и законные интересы третьих лиц.

5.3 Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона N 261-ФЗ, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

5.4 В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона N 261-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

5.5 Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для

заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

5.6 Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

6.Обеспечения защиты персональных данных, хранящихся в личных делах работников

6.1 В целях обеспечения защиты персональных данных, хранящихся в личных делах работников Оператора, работники имеют право:

– получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

– осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных Федеральным законом «О персональных данных»;

– требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением Федеральных законов. Сотрудник при отказе Оператора исключить или исправить его персональные данные имеет право заявить в письменной форме работодателю о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения;

– требовать от работодателя уведомления всех лиц, которым ранее были сообщены неверные или неполные их персональные данные, обо всех произведенных в них изменениях или исключениях из них;

– обжаловать действия или бездействие работодателя в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если гражданский служащий, являющийся субъектом персональных данных, считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы.

6.2 В целях обеспечения достоверности персональных данных, хранящихся в личных делах работников, работники обязаны:

6.2.1 передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен ТК РФ;

6.2.2 при изменении сведений, содержащих персональные данные (фамилия, имя, отчество, адрес, паспортные данные, сведения об образовании, семейном положении, состоянии здоровья, при выявлении противопоказаний для

выполнения служебных обязанностей), своевременно (как правило, в 3-дневный срок) сообщать о таких изменениях.

7 Порядок приостановки предоставления ПДн в случае обнаружения нарушения порядка их предоставления

7.1 В случае обнаружения нарушений порядка предоставления ПДн ответственным за обеспечение безопасности ПДн Оператор приостанавливает обработку ПДн до выяснения и устранения причин нарушений.

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

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

8.1 Запросы пользователей информационных систем ПДн Оператора 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.

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

9 Правила парольной защиты

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

9.1.1 по паролю условно-постоянного действия, длиной не менее семи буквенно-цифровых символов;

9.1.2 с использованием электронного идентификатора, который служит для авторизации пользователя на компьютерах с установленным СЗИ.

9.2 Персональные пароли должны выбираться следующих требований:

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

9.2.2 при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 (2,3..,7,8) позициях;

9.2.3 личный пароль пользователь не имеет права сообщать никому;

9.2.4 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, abcd 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.

9.3 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.).

9.4 Порядок смены личных паролей:

9.4.1 смена паролей должна проводиться регулярно, не реже 1 раза в 3 месяца.

9.4.2 в случае прекращения полномочий пользователя (увольнение, либо переход на другую работу) производится немедленное удаление его идентификационных данных.

9.4.3 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.

9.4.4 администратор ведет "Журнал принудительной смены личных паролей", в котором отмечает причины внеплановой смены паролей пользователей.

9.4.5 временный пароль, заданный администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

9.5 Хранение пароля.

9.5.1 запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

9.5.2 запрещается оставлять без присмотра рабочее место с незаблокированным монитором;

9.5.3 запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

9.5.4 хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у администратора или руководителя подразделения.

9.6 Ответственность при организации парольной защиты.

9.6.1 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.

9.6.2 ответственность за организацию парольной защиты в организации возлагается на администраторов.

9.6.3 периодический контроль за соблюдением требований парольной защиты возлагается на техника В.А. Ветлицина.

9.7 В том случае, если на ПК пользователя установлено СЗИ, не оснащенная электронными идентификаторами, то пароль записывается в персональный идентификатор пользователя. в идентификатор записывается имя оснащенное паролем, пользователь осуществляет вход в систему с использованием идентификатора. Идентификатор также может хранить в своей памяти и криптоключ пользователя. Запись пароля в идентификатор производится администратором:

9.7.1 администратор производит генерацию новых паролей к учетным записям и выдачу ключей пользователям;

9.7.2 администратор осуществляет запись криптографического ключа в идентификатор пользователя.

9.8 Устанавливаются следующие парольные политики:

Политика	Параметр безопасности
Максимальный срок действия пароля	3 месяца
Минимальная длина пароля	7 символов
Минимальный 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

9.9 Пользователь, получивший электронный идентификатор для доступа к ИСПДн, обязан:

9.9.1 обязательно использовать идентификатор для входа в систему;

9.9.2 не передавать идентификатор другим пользователям;

9.9.3 хранить идентификатор в “надежном месте” – например на связке ключей, в сейфе, в шкафу;

9.9.4 не хранить идентификатор рядом со считывателем, на столе\системном блоке, в первом ящике стола, на видном месте;

9.9.5 бережно хранить идентификатор, избегать падений идентификатора, воздействий сильных электромагнитных полей, попадания жидкости на идентификатор;

9.9.6 если идентификатор содержит криптоключ, быть аккуратным при шифровании и расшифровке папок и файлов;

9.9.7 в случае утери идентификатора немедленно сообщить об этом одному из администраторов информационной безопасности, а в случае их отсутствия – администраторам.

9.10 Порядок хранения и смены личных паролей:

9.10.1смена 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;

9.10.2смену пароля производит администратор;

9.10.3список паролей пользователей хранится у администраторов;

9.10.4изменение пароля производится локально, пользователь должен принести ключ администратору для смены пароля, администратор изменяет пароль пользователя и записывает новый пароль в идентификатор;

9.10.5администратор, 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.

10 Правила антивирусной защиты

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

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

10.3 Пользователям ИСПДн запрещено самостоятельное копирование и установка ПО любого назначения. Копирование или установка какого-либо ПО должны производиться исключительно администратором ИБ.

10.4 Для правильной работы необходимо:

10.4.1настроить внутренний планировщик антивирусного ПО на автоматическую загрузку обновлений. При невозможности автоматической загрузки ежедневно производить загрузку обновлений антивирусного ПО и производить обновления.

10.4.2настройку антивирусного ПО выполнить в соответствии с утвержденным «Регламентом настройки политик безопасности при эксплуатации СЗИ».

10.4.3не запускать файлы, полученные от ненадежного источника, прежде чем они не будут проверены антивирусной программой с последними обновлениями.

10.4.4в обязательном порядке проверять антивирусным ПО все внешние накопители информации (оптические диски, флэш-накопители, карты памяти, сменные и внешние жесткие диски).

11 Правила обновления общесистемного и прикладного программного обеспечения ИСПДн

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

11.1.1изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);

11.1.2изменился состав угроз безопасности ПДн в ИСПДн;

11.1.3изменился класс ИСПДн.

11.2 Обновления общесистемного и прикладного программного обеспечения ИСПДн осуществляются под контролем техника-программиста В.А. ВЕтлицина при необходимости – специализированных организаций.

12 Порядок обучения администраторов ИСПДн

12.1 Оператор не реже одного раза в год проводит обучение администраторов ИСПДн по вопросам информационной безопасности с доведением под подпись требований нормативных документов по защите ПДн.

13 Требования к помещениям, в которых располагаются ИСПДн

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

13.2 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».

13.3 Помещения ограниченного доступа должны располагаться в контролируемой зоне.

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

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

13.6 В случае, когда помещения ограниченного доступа располагаются на первых и последних этажах здания, их окна должны быть оснащены сигнализацией.

13.7 Двери помещений ограниченного доступа не должны отличаться от дверей других помещений и не должны иметь обозначающих и предупреждающих надписей и табличек.

13.8 Внутренняя планировка и расположение рабочих мест в помещениях ограниченного доступа должны обеспечивать исполнителям работ недоступность и сохранность доверенных им ПДн.

13.9 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.

13.10 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:

13.10.1 помещение должно располагаться в контролируемой зоне;

13.10.2 двери помещения должны иметь надежные запоры, приспособления для опечатывания, либо должны быть оснащены контроллерами, включенными в систему контроля ограничения доступа;

13.10.3 желательно наличие видеокамеры включенной в систему видеозаписи, контролирующей вход в помещение;

13.10.4 должны быть задействованы все меры, исключающие неконтролируемое пребывание в помещении любых лиц, включая сотрудников организации, не допущенных к работе с ПДн;

13.10.5 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;

13.10.6 помещение должно быть оборудовано средствами пожаротушения, желательно наличие автономной автоматической системы пожаротушения;

13.10.7 помещение должно быть оборудовано необходимым количеством стеллажей и/или шкафов для хранения архивных носителей;

13.10.8 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);

13.10.9 от двери помещения должны быть резервные ключи;

13.10.10 помещение, предназначенное для хранения резервных копий, не должно совмещаться с помещением, в котором размещается оборудование, создающее и (или) использующее указанные резервные копии.

13.10.11 размещение в помещении оборудования и вспомогательных технических средств должно отвечать санитарно-гигиеническим нормам, а также требованиям техники безопасности и пожарной безопасности.

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

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

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

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

14.1 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.

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

14.3 Основаниями для назначения служебной проверки являются устное заявление, докладная или служебная записка работника ГБУЗ СО «ГП № 3 г. Нижний Тагил», а также выявление факта одного или нескольких нарушений.

14.4 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.

14.5 В состав комиссии в обязательном порядке входят:

14.5.1председатель комиссии – ответственный за обеспечение безопасности ПДн.

14.5.2члены комиссии – специалисты по разработке и осуществлению мероприятий по организации и обеспечению безопасности ПДн при их обработке в информационных системах персональных данных

14.6 В случае необходимости председатель комиссии может привлекать к работе:

14.6.1непосредственного начальника нарушителя;

14.6.2экспертов из других подразделений:

14.6.3специалистов организаций-лицензиатов.

14.7 Члены комиссии имеют право:

14.7.1требовать документального подтверждения факта нарушений информационной безопасности ИСПДн;

14.7.2устанавливать причины допущенных нарушений любым из способов, не противоречащих законодательству РФ;

14.7.3брать письменные объяснения по поводу выявленных нарушений у любого сотрудника ГБУЗ СО «ГП № 3 г. Нижний Тагил».

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

14.8.1документальное подтверждение факта нарушений ИБ ИСПДн;

14.8.2установленные причины выявленных нарушений в ИБ ИСПДн;

14.8.3предложения по устранению причин выявленных инцидентов ИБ в ИСПДн;

14.8.4предложения по дополнению Перечня нарушений ИБ.

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

15 Перечень нарушений ИБ ИСПДн

15.1 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:

15.1.1несанкционированная переконфигурация параметров ИСПДн;

15.1.2утрата или кража резервной копии базы данных ИСПДн;

15.1.3необоснованная передача базы данных ИСПДн;

15.1.4организация утечки ПДн ИСПДн по техническим каналам;

15.1.5умышленное нарушение работоспособности ИСПДн;

15.1.6НСД к ПДн ИСПДн;

15.1.7несанкционированное внесение изменений в базу данных ИСПДн;

15.1.8умышленное заражение компьютеров и серверов ИСПДн вирусами;

15.1.9проведение работ с ИСПДн, повлекшее за собой необратимую потерю данных;

15.1.10 другие действия, подпадающие под действия статей 272, 273, 274 УК РФ.

15.2 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:

15.2.1 подбор административного пароля (успешный);

15.2.2ошибка при входе в ИСПДн (набор не назначенного пароля, более трех раз подряд, периодически);

15.2.3несанкционированное (неоднократное) оставление включенного ПК;

15.2.4утрата учтенного отчуждаемого съемного носителя;

15.2.5попытка входа под чужим именем, паролем, многократная неудачная;

15.2.6попытка входа под чужим именем, паролем, удачная;

15.2.7несанкционированная очистка журналов аудита;

15.2.8несанкционированное копирование ПДн на внешние носители;

15.2.9несанкционированная установка (удаление) ПО на ПК ИСПДн;

15.2.10 несанкционированное изменение конфигурации ПО ПК ИСПДн;

15.2.11 попытка получения прав администратора на локальном ПК (увеличения собственных прав, получение прав на отладку программ), удачная и неудачная;

15.2.12 попытка получения прав администратора в домене или на удаленной машине, удачная и неудачная;

15.2.13 неумышленное заражение локального или сетевого ПК компьютерными вирусами.

15.2.14 несанкционированное использование сканирующего ПО;

15.2.15 несанкционированное использование анализаторов протоколов (снифферов);

15.2.16 несанкционированный просмотр, вывод на печать ПДн.

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

15.3.1ошибка при входе в ИСПДн (набор неправильного пароля, сетевого имени более трех раз подряд);

15.3.2попытка неудачного доступа к ПДн ИСПДн (периодическая);

15.3.3перевод времени на ПК;

15.3.4работа на ПК в неразрешенное время;

15.3.5перезагрузка компьютера при сбоях в работе ПК (однократная), в т.ч. аварийная перезагрузка, путем нажатия кнопки RESET;

15.3.6нецелевое использование корпоративных ресурсов (печать, Internet, mail, и др).

16 Порядок контроля за соблюдением условий использования средств защиты информации

16.1 Контроль за соблюдением условий использования СЗИ осуществляет старший системный администратор ГБУЗ СО «МИАЦ» (620078, г. Екатеринбург, ул. Гагарина, дом 53) в соответствии с выработанным регламентом.

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

16.3 По результатам проверок составляется акт, при выявлении замечаний – предписание на устранение выявленных замечаний.

17 Государственный контроль и надзор за эксплуатацией аттестованных ИСПДн

17.1 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.

17.2 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.

17.3 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.

17.4 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.

17.5 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.

17.6 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.

18 Порядок взаимодействия с вышестоящими службами и федеральными органами

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

18.2 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»:

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

19 Общедоступные источники персональных данных сотрудников Оператора

19.1 В целях информационного обеспечения Оператором 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.

19.2 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.

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

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

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

20.2.1 руководитель, разрешающий доступ сотрудника к персональным данным несет персональную ответственность за данное разрешение;

20.2.2каждый сотрудник несет единоличную ответственность за сохранность носителей персональных данных и соблюдение конфиденциальности информации;

20.2.3 сотрудник ГБУЗ СО «ГП № 3 г. Нижний Тагил», разгласивший персональные данные пациента, предоставивший работодателю подложные документы или заведомо ложные сведения о себе, либо своевременно не сообщивший об изменениях персональных данных, несет дисциплинарную ответственность, вплоть до увольнения.

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