Приложение № 8

Положение
о защите персональных данных пациентов и работников ГАУЗ «СП» г. Бугуруслана

1. Общие положения

1.1. Настоящее Положение устанавливает требования и порядок обеспечения безопасности персональных данных пациентов и работников государственного автономного учреждения здравоохранения «Стоматологическая поликлиника» г.Бугуруслана (далее по тексту – Учреждение), а также права и обязанности пациентов и работников Учреждения.

1.2. Основанием для разработки настоящего положения:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 года №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 года №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСБ РФ от 10 июля 2014 года №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Устав Учреждения;
- Политика в отношении обработки персональных данных пациентов и работников в Учреждении;
- Положение об обработке персональных данных пациентов и работников Учреждения;
- приказы главного врача в сфере защиты персональных данных.

1.3. Целью настоящего Положения является:

- определение требований к защите персональных данных пациентов Учреждения, а также лиц, работающих по трудовым и гражданско-правовым договорам (далее – работников) Учреждения, согласно Перечню персональных данных, утвержденного приказом главного врача;
- определение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных пациентов и работников Учреждения при их

обработке в информационных системах персональных данных, в том числе с использованием средств криптографической защиты информации;

– установление ответственности должностных лиц, имеющих доступ к персональным данным пациентов и работников Учреждения за невыполнение требований и норм, регулирующих обработку и защиту персональных данных.

1.4. Персональные данные пациентов и работников относятся к категории конфиденциальной информации. Конфиденциальность, сохранность и защита персональных данных обеспечиваются отнесением их к сфере служебной тайны.

2. Основные понятия, используемые в настоящем Положении

В целях настоящего Положения применяются следующие термины и определения:

Пациенты (субъекты персональных данных) - физические лица, обратившиеся к Учреждению с целью получения медицинского обслуживания, либо состоящие в иных гражданско-правовых отношениях с Учреждением по вопросам получения медицинских услуг.

Работники (субъекты персональных данных) - физические лица, состоящие в трудовых и иных гражданско-правовых отношениях с Учреждением.

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

Документы, содержащие ПДн пациента - документы, необходимые для осуществления действий в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, а также для оформления договорных отношений.

Документы, содержащие ПДн работника - документы, которые работник предоставляет Учреждению (работодателю) в связи с трудовыми отношениями и касающиеся конкретного работника (субъекта ПДн), а также другие документы, содержащие сведения, предназначенные для использования в служебных целях.

Врачебная тайна - соблюдение конфиденциальности информации о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иных сведений, полученных при его обследовании и лечении.

Обработка ПДн пациента или работника - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление уничтожение ПДн пациента или работника.

Автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники.

Информационная система ПДн (ИСПДн) - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность ПДн - операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законодательством.

Целостность ПДн – обеспечение достоверности и полноты ПДн и методов их обработки.

Доступность ПДн – обеспечение доступа к ПДн пользователей при необходимости.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами ПДн.

Общедоступные ПДн - ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с Федеральным законодательством не распространяется требование соблюдения конфиденциальности.

Персональная электронно-вычислительная машина (ПЭВМ) – персональный компьютер работника Учреждения.

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

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

Защита ПДн – процесс обеспечения безопасности ПДн.

Идентификация – действия по присвоению субъектам и объектам доступа идентификаторов и сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Аутентификация – действия по проверке подлинности субъекта доступа в автоматизированной информационной системе.

Машинный носитель информации – любое техническое устройство либо физическое поле, предназначенное для фиксации, хранения, накопления, преобразования и передачи компьютерной информации.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Средство защиты информации – аппаратное, программное или аппаратно-программное средство, используемое для защиты информации.

Средство криптографической защиты информации (СКЗИ) – средство защиты информации, реализующие алгоритмы криптографического преобразования информации.

3. Общие положения по защите ПДн пациентов и работников

3.1 Меры по обеспечению безопасности ПДн реализуются в рамках системы защиты ПДн, создаваемой в соответствии с Требованиями к защите ПДн при их обработке в ИСПДн, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119, и направлены на нейтрализацию актуальных угроз безопасности ПДн.

Система защиты ПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИСПДн.

3.2 Выбор средств защиты информации для системы защиты ПДн осуществляется Учреждением в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона "О персональных данных".

3.3 Определение типа угроз безопасности ПДн, актуальных для ИСПДн, производится Учреждением с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона "О персональных данных".

3.4 Обеспечение безопасности ПДн пациентов и работников достигается, в частности:

а) определением угроз безопасности ПДн при их обработке в информационных

системах ПДн;

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

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

г) оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн;

д) учетом машинных носителей ПДн;

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

ж) восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

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

и) контролем над принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности информационных систем ПДн.

3.4.1 Организация обработки и защиты ПДн пациентов и работников Учреждения без использования средств автоматизации осуществляется в соответствии с законодательством Российской Федерации и Положением о порядке обработки ПДн, осуществляемой без использования средств автоматизации в Учреждении.

3.4.2 Организация автоматизированной обработки и защиты ПДн пациентов и работников Учреждения осуществляется в соответствии с законодательством Российской Федерации и Положением о защите ПДн пациентов и работников Учреждения.

3.5 Режим конфиденциальности ПДн снимается в случаях их обезличивания и по истечении срока их хранения, в соответствии с приказами главного врача Учреждения по архивному делу, или продлевается на основании заключения экспертной комиссии Учреждения, если иное не определено действующим законодательством Российской Федерации.

4 Обеспечения защиты ПДн пациентов и работников при их обработке ИСПДн

4.1 Система защиты ПДн строится в соответствии постановлению Правительства Российской Федерации от 1 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», опираясь на уровень защищенности ПДн при их обработке в ИСПДн.

4.2 Для определения уровня защищенности ПДн, обрабатываемых в ИСПДн, создается специальная экспертная группа, которая формирует предварительный перечень ИСПДн для классификации по уровню защищенности ПДн.

Комиссия соблюдает следующий порядок классификации ИСПДн:

4.2.1 Определяется категория ИСПДн. Основанием для категорирования ИСПДн является составленный экспертной группой перечень ПДн, содержащий информацию о категориях обрабатываемых ПДн, субъектах ПДн (работники Учреждения, пациенты, временные посетители) и их количестве.

4.2.2 Определяется тип актуальных угроз для ИСПДн, формируемый на основе перечня актуальных угроз безопасности ИСПДн.

Данный перечень также составляет экспертная группа, основываясь на оценке возможности реализации угроз безопасности ИСПДн, которая формируется из уровня исходной защищенности ИСПДн и вероятности реализации угроз.

Уровень исходной защищенности ИСПДн определяется как обобщенный степенной

показатель (низкий, средний, высокий), зависящий от технических и эксплуатационных характеристик ИСПДн. Вероятность реализации угрозы безопасности ПДн определяется методом опроса экспертной группы. В опрос включаются угрозы из базовой модели угроз безопасности с учетом технических и эксплуатационных характеристик ИСПДн. Эксперты выносят вердикт о вероятности и опасности угрозы безопасности ПДн, после чего определяется коэффициент ее реализуемости и актуальность.

В случае если в перечень угроз безопасности ИСПДн входят угрозы, нейтрализуемые только с помощью СКЗИ, определение актуальности данного типа угроз производится в соответствии порядку, установленному методическими рекомендациями ФСБ РФ от 31 марта 2015 года «По разработке нормативно-правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности».

4.2.3 На основании определенных категории ИСПДн и типа актуальных угроз устанавливается один из 4-х уровней защищенности ПДн при их обработке в ИСПДн. Для обеспечения определенного уровня защищенности ПДн выдвигаются требования к защите ПДн при их обработке в ИСПДн.

4.3 Установленные уровни защищенности ПДн для всех ИСПДн Учреждения являются основанием для выбора организационных и технических мер по защите ПДн. Выбор мер по обеспечению безопасности ПДн, подлежащих реализации в ИСПДн в рамках системы защиты ПДн, включает в себя следующие этапы:

4.3.1 Определяется базовый набор мер по обеспечению безопасности ПДн для установленного уровня защищенности ПДн в соответствии с базовыми наборами мер по обеспечению безопасности ПДн, приведенными в приложении к Приказу ФСТЭК России от 18 февраля 2013 года №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Приказ ФСТЭК №21);

4.3.2 Адаптируется базовый набор мер по обеспечению безопасности ПДн с учетом структурно-функциональных характеристик ИСПДн, информационных технологий, особенностей функционирования ИСПДн (в том числе исключается из базового набора меры, непосредственно связанные с информационными технологиями, не используемыми в ИСПДн, или структурно-функциональными характеристиками, не свойственными ИСПДн);

4.3.3 Уточняется адаптированный базовый набор мер по обеспечению безопасности ПДн с учетом не выбранных ранее мер, приведенных в приложении к Приказу ФСТЭК №21, в результате чего определяются меры по обеспечению безопасности ПДн, направленные на нейтрализацию всех актуальных угроз безопасности ПДн для конкретной ИСПДн;

4.3.4 Дополняется уточненный адаптированный базовый набор мер по обеспечению безопасности ПДн мерами, обеспечивающими выполнение требований к защите ПДн, установленными иными нормативными правовыми актами в области обеспечения безопасности ПДн и защиты информации.

4.3.5 В случае актуальности для ИСПДн 1-го и 2-го типа угроз безопасности ПДн, дополнительно к мерам по обеспечению безопасности ПДн могут применяться меры:

–проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

–тестирование информационной системы на проникновения;

–использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

4.3.6 При использовании в ИСПДн сертифицированных по требованиям безопасности информации средств защиты информации для обеспечения уровня

защищенности ПДн конкретной ИСПДн Учреждения учитывается соответствие класса средства защиты информации требованиям Приказа ФСТЭК №21.

4.3.7 При использовании в ИСПДн сертифицированных по требованиям безопасности информации СКЗИ для обеспечения уровня защищенности ПДн конкретной ИСПДн Учреждения проводятся мероприятия, указанные в пункте 4.2.4 настоящего Положения и определяется класс СКЗИ в соответствии с Приказом ФСБ РФ от 10 июля 2014 №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

4.4 В общем случае при обработке ПДн в ИСПДн система защиты ПДн в Учреждении должна обеспечивать:

а) идентификацию и аутентификацию субъектов и объектов доступа ИСПДн;
б) управление доступом субъектов и объектов доступа;
в) ограничение программной среды;
г) защиту машинных носителей ПДн;
д) регистрацию событий безопасности;
е) антивирусную защиту;
ж) обнаружение вторжений;
з) контроль защищенности ПДн;
и) целостность ИСПДн;
к) доступность ПДн;
л) защиту среды виртуализации;
м) защиту технических средств;
н) защиту ИСПДн, ее средств, систем связи и передачи данных;
о) выявление инцидентов безопасности и реагирование на них;
п) управление конфигурацией ИСПДн и системы защиты ПДн.

Состав и содержание мер по обеспечению безопасности ПДн, необходимых для обеспечения каждого из уровней защищенности ПДн, устанавливаются экспертной группой.

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

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

Доступ сотрудников к ИСПДн Учреждения осуществляется в соответствии перечню лиц, допущенных к работе в ИСПДн. Данный перечень формируется приказом главного врача Учреждения.

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

4.4.4 Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных

данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

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

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

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

4.4.8 Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

4.4.9 Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

4.4.10 Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

4.4.11 Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

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

4.4.13 Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения

архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

4.4.14 Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

4.4.15 Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

4.5 На основании сформированного перечня классифицированных ИСПДн составляются частные модели угроз, описывающие основные угрозы безопасности ПДн, в целях уточнения или построения системы защиты информации.

5 Обеспечение защиты ПДн пациентов и работников с использованием СКЗИ

5.1 Безопасность обработки ПДн с использованием СКЗИ организует и обеспечивает ответственный пользователь СКЗИ Учреждения и лица, которым на основании приказа главного врача Учреждения дается право на обработку персональных данных с использованием СКЗИ.

5.2 Учреждение и пользователи СКЗИ несут ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности ПДн при их обработке с использованием СКЗИ лицензионным требованиям и условиям, эксплуатационной и технической документации к СКЗИ. При этом Учреждение и ответственный пользователь должны обеспечивать комплексность защиты ПДн, в том числе посредством применения иных средств защиты информации.

5.3 При разработке и реализации мероприятий по организации и обеспечению безопасности персональных данных при их обработке в ИСПДн Учреждение и ответственный пользователь СКЗИ осуществляют:

– разработку для каждой ИСПДн модели угроз безопасности ПДн;

– определение необходимости использования СКЗИ для обеспечения безопасности ПДн и, в случае положительного решения, определение на основе модели угроз цели использования СКЗИ для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн и (или) иных неправомерных действий при их обработке;

– установку и ввод в эксплуатацию СКЗИ в соответствии с эксплуатационной и технической документацией;

– проверку готовности СКЗИ к использованию с составлением заключений о возможности их эксплуатации;

– обучение лиц, использующих СКЗИ, работе с ними;

– поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним, носителей ПДн;

– учет лиц, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности ПДн в ИСПДн (пользователи СКЗИ);

– контроль за соблюдением условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией;

– разбирательство и составление заключений по фактам нарушения условий хранения носителей ПДн, использования СКЗИ, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

– описание организационных и технических мер, которые Учреждение будет

осуществлять при обеспечении безопасности ПДн с использованием СКЗИ при их обработке в ИСПДн, с указанием в частности:

а) индекса, условного наименования и регистрационных номеров используемых СКЗИ;

б) соответствия размещения и монтажа аппаратуры и оборудования, входящего в состав СКЗИ, требованиям нормативной документации и правилам пользования СКЗИ;

в) соответствия помещений, в котором размещены СКЗИ и хранится ключевая документация.

5.4 Пользователи СКЗИ допускаются к работе с СКЗИ на основании приказа главного врача Учреждения. При наличии двух и более пользователей СКЗИ, работающих в одной и той же ИСПДн, обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность СКЗИ, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

5.5 Пользователи СКЗИ обязаны:

– не разглашать информацию, к которой они допущены, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты;

– соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности СКЗИ и ключевых документов к ним;

– сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

– немедленно уведомлять ответственного пользователя СКЗИ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

– сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

5.6 Обеспечение функционирования и безопасности СКЗИ возлагается на ответственного пользователя СКЗИ, имеющего необходимый уровень квалификации, назначаемого приказом главного врача Учреждения.

5.7 Допускается возложение функций ответственного пользователя СКЗИ на:

– одного из пользователей СКЗИ;

– на структурное подразделение или должностное лицо (работника), ответственных за обеспечение безопасности ПДн;

– на специальное структурное подразделение по защите информации, использующее для этого СКЗИ.

5.8 Ответственные пользователи СКЗИ должны иметь функциональные обязанности, разработанные в соответствии с настоящим Положением.

5.9 Лица, назначенные пользователями (ответственными пользователями) СКЗИ, должны быть ознакомлены с соответствующими инструкциями, настоящим Положением и другими документами, регламентирующими организацию и обеспечение безопасности ПДн при их обработке в ИСПДн, под роспись и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством Российской Федерации.

5.10 Текущий контроль за организацией и обеспечением функционирования СКЗИ возлагается на ответственного пользователя СКЗИ в пределах его служебных полномочий.

5.11 Контроль за организацией, обеспечением функционирования и безопасности СКЗИ, предназначенных для защиты ПДн при их обработке в ИСПДн, осуществляется в соответствии с действующим законодательством Российской Федерации.

5.12 При обеспечении безопасности ПДн при их обработке в ИСПДн с использованием СКЗИ приказом главного врача Учреждения назначается ответственный

пользователь СКЗИ, указания которого являются обязательными для всех пользователей СКЗИ.

5.13 Организации, оказывающие возмездные услуги Учреждению в области криптографической защиты информации должны иметь действующую лицензию ФСБ России на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

5.14 Лицензиаты ФСБ России несут ответственность за соответствие проводимых ими работ и услуг, лицензионным требованиям и условиям, эксплуатационной и технической документации к СКЗИ.

6 Обеспечение защиты ПДн пациентов и работников при их обработке без использования средств автоматизации

6.1 Для обеспечения безопасности ПДн при неавтоматизированной обработке предпринимаются следующие меры:

6.1.1 Обработка ПДн, осуществляемая без использования средств автоматизации, осуществляется с определением места хранения ПДн (материальных носителей) для каждой категории ПДн и перечнем лиц, допущенных к неавтоматизированной обработке ПДн.

6.1.2 Обеспечивается раздельное хранение ПДн и материальных носителей ПДн, обработка которых осуществляется в различных целях.

6.1.3 При хранении материальных носителей обеспечивается сохранность и исключение несанкционированного доступа:

6.1.3.1 В кабинетах, где осуществляется хранение материальных носителей, содержащих ПДн, имеются сейфы, шкафы, стеллажи, тумбы;

6.1.3.2 Кабинеты, где осуществляется хранение материальных носителей ПДн, оборудованы замками и системами охранной и пожарной сигнализации;

6.1.3.3 Учреждение использует услуги вневедомственной охраны.

6.2 Не допускается копирование информации с журналов, содержащих ПДн, необходимые для однократного пропуска субъекта ПДн на территорию Учреждения, или в иных аналогичных целях.

7 Обязанности Учреждения по защите ПДн пациентов и работников

7.1 Учреждение при обработке ПДн пациентов и работников обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

7.2 Учреждением назначается лицо, ответственное за организацию обработки ПДн.

7.3 Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

– осуществлять внутренний контроль за соблюдением оператором и его

работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

8 Ответственность за нарушение норм, регулирующих обработку и защиту ПДн пациентов и работников

8.1 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн пациента и работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

8.2 Работники Учреждения, допущенные к обработке ПДн пациентов и работников, за разглашение полученной в ходе своей трудовой деятельности информации, несут дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

9 Заключительные положения

9.1 Настоящее Положение вступает в силу с даты его утверждения.

9.2 Настоящее положение распространяется на всех лиц Учреждения, допущенных к обработке ПДн.

9.3 Работники Учреждения подлежат ознакомлению с данным документом в порядке, предусмотренном приказом главного врача Учреждения под личную подпись.