Экз. № 1

УТВЕРЖДАЮ
Главный врач
ГАУЗ «КЭД»
_____Г.А. Гильманова
«___» _____2019 г.

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГАУЗ «КЭД»

Настоящее Положение разработано в соответствии с Федеральным Законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативными документами ФСТЭК и ФСБ России с целью обеспечения защиты прав и свобод граждан при обработке их персональных данных в информационных системах персональных данных.

Для целей настоящего Положения применяются следующие термины и определения:

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

Оператор Персональных данных – Государственное автономное учреждение здравоохранения «Казанский эндокринологический диспансер» (далее Учреждение) – 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.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи,

звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа к информационным системам персональных данных – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу 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.

Конфиденциальность персональных данных – Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Несанкционированный доступ (несанкционированные действия) к информационным системам персональных данных – доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

Защита информации – комплекс организационно-технических мероприятий, направленных на предотвращение потери, искажения и несанкционированного доступа к данным, при этом предусматривается:

- разграничение полномочий доступа к данным;
- авторизация, контроль и учет действий с данными (регистрация событий);
- контроль копирования, печати, обмена данными по каналам связи;
- межсетевое экранирование и защита от вирусов;
- учет внешних носителей данных;
- резервное копирование / восстановление данных;
- раздельное хранение носителей данных с резервными копиями;
- контроль доступа в помещения и к компьютерам;
- применение устройств идентификации пользователей для доступа.

1 Общие положения

Настоящим Положением определяется структура и составляющие безопасности информации в информационной системе персональных данных работников и пациентов Учреждения.

Обеспечение безопасности персональных данных (ПДн) при их обработке в автоматизированных системах (информационных системах персональных данных – ИСПДн) достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

Мероприятия по обеспечению безопасности ПДн формулируются на основании анализа типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, Учреждения и государства.

Обеспечение безопасности ПДн осуществляется путем выполнения Требований по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения

(Приложение № 1).

Структура, состав и основные функции СЗПДн определяются исходя из анализа типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности осуществляемых на всех стадиях жизненного цикла ИСПДн согласованных по цели, задачам, месту и времени мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн; на восстановление нормального функционирования ИСПДн после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз.

Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего уровня защищенности информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию разрешенных лицензионных средств защиты информации в соответствии с эксплуатационной и технической документацией;

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

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

ж) учет лиц, допущенных к работе с ПДн в информационной системе;

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

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, 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;

к) описание системы защиты персональных данных.

Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности ПДн при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

По структуре ИСПДн, на которые направлена реализация мероприятий по защите, выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автоматизированного рабочего места;
- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем;
- угрозы, реализуемые в ИСПДн при их подключении к сетям связи общего пользования.

Для обеспечения безопасности ПДн при их обработке в информационных системах проводятся:

- обследование и оформление документа о типе актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн, определение способов и состава средств защиты информации (СЗИ), разработка технического задания (ТЗ) на создание комплексной системы защиты информации, в том числе разработка модели угроз, проектирование;
- ввод в эксплуатацию – закупка и инсталляция сертифицированных СЗИ, обучение персонала, издание приказов о допуске персонала и регламентов обработки конфиденциальной информации.

2 Цели обеспечения информационной безопасности

Стратегической целью обеспечения безопасности информации в ИСПДн является защита интересов субъектов информационных отношений. Данная цель достигается посредством постоянного поддержания следующих свойств информации в процессе ее обработки, хранения и передачи:

- целостности информации;
- доступности обрабатываемой информации для зарегистрированных пользователей;
- конфиденциальности информации.

3 Объект защиты

Объектом защиты является информационная система персональных данных работников и пациентов Учреждения:

а) Информационные ресурсы:

- персональные данные работников и пациентов (исходная информация, информационные базы данных);
- инструментальная информация (программное обеспечение), с помощью которой обрабатывается, хранится и передается информация ПДн;

б) технические информационные системы и средства Учреждения, в которых обрабатывается, хранится и передается информация ПДн;

в) помещения объектов Учреждения, в которых размещаются информационные ресурсы, и обрабатывается конфиденциальная информация;

г) технические системы жизнеобеспечения, электропитания, проводного вещания, охранной сигнализации, обеспечивающие или размещаемые совместно с оборудованием ИСПДн.

Критичными свойствами объекта защиты являются:

а) возможность разрушения или повреждения информационных систем персональных данных в результате пожара, затопления, аварии инженерных систем жизнеобеспечения;

б) возможность прекращения или нарушения нормального функционирования ИСПДн в результате повреждения отдельных их элементов;

в) несанкционированная доступность информации, выражающаяся в возможности:

- непосредственного доступа к информации, находящейся на первичном или вторичном носителе, в транспортной среде передачи; воздействия на носитель или транспортную среду с целью перлюстрации, отчуждения, копирования, изменения, подмены и уничтожения информации;

- прямого или косвенного доступа к оборудованию ИСПДн и транспортной среде передачи с целью получения доступа к информации (несанкционированный доступ);
- перехвата речевой информации по акустическим и другим каналам утечки (подслушивание).

4 Субъекты информационных отношений

4.1 Субъектами информационных отношений являются:

- Работники ((субъекты персональных данных) - физические лица, вступившие, а также готовящиеся вступить в трудовые и иные гражданско-правовые отношения, не состоящие в трудовых отношениях с Учреждением-оператором (уволенные работники, кандидаты на вакантные должности, родственники работников);
- Пациенты (субъекты персональных данных) - физические лица, которым оказывается медицинская помощь или которые обратились за оказанием медицинской помощи в Учреждение-оператор, независимо от наличия у них заболевания и от их состояния, либо состоящие в иных гражданско-правовых отношениях с Учреждением-оператором по вопросам получения медицинских услуг.

4.2 Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- конфиденциальности (сохранения в тайне) информации в соответствии с требованиями российского законодательства;
- достоверности (полноты, точности, адекватности, целостности) информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);
- своевременного доступа (за приемлемое для них время) к необходимой им информации;
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
- защиты информации от незаконного ее тиражирования (защиты персональных данных, защиты авторских прав, прав собственника информации).

5 Возможные угрозы и участки вторжения

Общая классификация угроз.

1. Угрозы конфиденциальности данных и программ. Реализуются при несанкционированном доступе к программам, данным, каналам связи, при перехвате электромагнитных излучений, при анализе трафика.

2. Угрозы целостности данных, программ, аппаратуры. Реализуются при несанкционированном уничтожении, модификации данных, порождении фальсифицированных данных, задержке и нарушении маршрутизации данных в каналах связи.

3. Угрозы доступности данных. Реализуются при создании условий, когда законный пользователь или процесс не получает своевременного доступа к данным или ресурсам системы, каналам связи.

6 Порядок проведения контрольных мероприятий и действий по результатам контроля

Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер. Контроль может проводиться комиссией, созданной в Учреждении, или на договорной основе сторонними организациями, при наличии лицензии на деятельность по технической защите конфиденциальной информации.

Решение основных вопросов обеспечения защиты ПДн предусматривает подготовку кадров, выделение необходимых финансовых и материальных средств, закупку программного и аппаратного обеспечения, а также, при необходимости, привлечение сторонней организации при наличии лицензий ФСТЭК и ФСБ.

Приложения к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГАУЗ «КЭД» являются самостоятельными документами и его неотъемлемой частью.

Список приложений:

Приложение № 1. Требования по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГАУЗ «КЭД».

Приложение № 2. Описание локально-вычислительной сети ГАУЗ «КЭД».

Приложение № 3. Описание состава технических средств ГАУЗ «КЭД», участвующих в обработке персональных данных.

Приложение № 4. Сведения о программном обеспечении ГАУЗ «КЭД», установленном на серверах и рабочих станциях, участвующих в обработке персональных данных.

Приложение № 5. Сведения о программно-технических средствах защиты ГАУЗ «КЭД», установленных на серверах и рабочих станциях, участвующих в обработке персональных данных.

Приложение № 6. Рекомендации по использованию программных и аппаратных средств защиты информации и обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Приложение № 1
к Положению по организации и
проведению работ по обеспечению
безопасности персональных данных
при их обработке в информационных
системах персональных данных
ГАУЗ «КЭД»

ТРЕБОВАНИЯ
по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГАУЗ «КЭД»

При организации и осуществлении защиты персональных данных (ПДн) необходимо руководствоваться требованиями нормативных и методических документов по защите информации в автоматизированных системах (информационных системах персональных данных – ИСПДн), учитывая при этом, что ПДн, в соответствии с Федеральным Законом от 27 июля 2006 года № 152 – ФЗ «О персональных данных» и Указом Президента РФ № 188 от 06.03.97 г., отнесены к конфиденциальной информации.

Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор 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.

2. Обеспечение 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.

При проведении мероприятий по защите ПДн учитывается, что информационные ресурсы подвержены потенциальным внешним и внутренним угрозам, ведущим к потерям конфиденциальности, доступности и целостности информационных ресурсов.

Источники угрозы:

- люди (недобросовестные внешние и внутренние пользователи информационных ресурсов);
- аварии (ошибки пользователя, ошибки администратора);
- отказ аппаратного обеспечения (ошибки программного обеспечения, отказы индустриального оборудования);
- природные факторы (стихийные бедствия, астрофизические явления, биологические явления).

Угрозы увеличивают риски безопасности, представляющие собой:

- неавторизированный доступ в сеть;
- неавторизированное раскрытие информации;
- неавторизированную модификацию данных или программного обеспечения;
- разрушение функций сети (недоступность данных и сервисов).

Наличие рисков безопасности требуют введения мер безопасности. Меры безопасности должны гарантировать:

- конфиденциальность;
- целостность;
- доступность информации;
- своевременное получение отчетности;
- физическую безопасность информации;
- контроль доступа к информации.

Информационная безопасность предусматривает:

- процедурную (административную и организационную безопасность);
- безопасность персонала;
- физическую безопасность;
- безопасность системы;
- безопасность коммуникаций.

Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

Мероприятия по обеспечению безопасности ПДн проводятся в зависимости от типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн, с учетом возможного возникновения угроз безопасности жизненно важным интересам субъектов персональных данных.

При обеспечении безопасности ПДн проводятся мероприятия, направленные на:

- предотвращение несанкционированного доступа (НСД) к ПДн и (или) передачи их лицам, организациям, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов НСД к ПДн;
- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- оперативного резервирования информации в ИСПДн;
- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;
- постоянный контроль за обеспечением уровня защищенности ПДн.

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных (СЗПДн).

Структура, состав и основные функции СЗПДн определяются в зависимости от типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн, используемых в Учреждении.

СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности осуществляемых на всех стадиях жизненного цикла ИСПДн согласованных по цели, задачам, месту и времени мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн, на восстановление нормального функционирования ИСПДн после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз. Обеспечение безопасности ПДн при их обработке в автоматизированных ИСПДн проводится путем выполнения комплекса организационных и технических мероприятий (применения технических средств), в рамках системы (подсистемы) защиты персональных данных, развертываемой в ИСПДн в процессе ее создания или модернизации.

Порядок организации обеспечения безопасности ПДн в ИСПДн предусматривает:

- оценку обстановки;
- обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн;
- разработку проекта обеспечения безопасности ПДн; выбор целесообразных способов (мер и средств) защиты ПДн в соответствии с задачами и проектом защиты;
- решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты;
- обеспечение реализации принятого проекта защиты;
- планирование мероприятий по защите ПДн;
- организацию и проведение работ по созданию системы защиты персональных данных (СЗПДн) в рамках разработки (модернизации) ИСПДн, в том числе с привлечением специализированных сторонних организаций к разработке и развертыванию СЗПДн или ее элементов в ИСПДн, решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации ИСПДн;
- разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн.

В интересах технического обеспечения безопасности ПДн при их обработке в ИСПДн, в зависимости от класса информационной системы должны быть проведены мероприятия по защите от НСД к ПДн при их обработке в ИСПДн.

В состав мероприятий по защите ПДн при их обработке в ИСПДн от НСД и неправомерных действий входят следующие мероприятия:

- защита от НСД при однопользовательском режиме обработки ПДн;
- защита от НСД при многопользовательском режиме обработки ПДн и равных правах доступа к ним субъектов доступа;

- защита от НСД при многопользовательском режиме обработки ПДн и разных правах доступа;
- защита информации при межсетевом взаимодействии ИСПДн;
- антивирусная защита.

Мероприятия по защите ПДн реализуются в рамках подсистем: управления доступом, регистрации и учета, обеспечения целостности, криптографической защиты, антивирусной защиты.

Меры безопасности ПДн должны гарантировать:

- конфиденциальность;
- целостность;
- доступность информации.

Мероприятия по обеспечению безопасности предусматривают:

- управление доступом;
- регистрацию и учет;
- обеспечение целостности;
- контроль отсутствия недекларированных возможностей;
- антивирусную защиту;
- обеспечение безопасного межсетевого взаимодействия;
- анализ защищенности.

Подсистемы управления доступом и регистрации и учета должны реализовываться на базе программных средств блокирования несанкционированных действий, сигнализации и регистрации. Это специальные, не входящие в ядро какой-либо операционной системы программные и программно-аппаратные средства защиты самих операционных систем, электронных баз данных и прикладных программ. Они выполняют функции защиты самостоятельно или в комплексе с другими средствами защиты и направлены на исключение или затруднение выполнения опасных действий пользователя или нарушителя.

Средства диагностики должны осуществлять тестирование файловой системы и баз данных, постоянный сбор информации о функционировании элементов подсистемы обеспечения безопасности информации.

Средства уничтожения предназначены для уничтожения остаточных данных и должны предусматривать аварийное уничтожение данных в случае угрозы несанкционированного доступа (НСД), которая не может быть блокирована системой.

Средства сигнализации предназначены для предупреждения операторов (пользователей) при их обращении к защищаемым данным и для предупреждения администратора при обнаружении факта НСД, искажении программных средств защиты, выходе или выводе из строя аппаратных средств защиты и о других фактах нарушения штатного режима функционирования.

Подсистема обеспечения целостности должна быть реализована операционными системами и системами управления базами данных. Средства повышения достоверности и обеспечения целостности передаваемых данных и надежности транзакций, встраиваемые в операционные системы и системы управления базами данных, основаны на расчете контрольных сумм, уведомлении о сбое в передаче пакета сообщения, повторе передачи не принятого пакета.

Подсистема контроля отсутствия недекларированных возможностей должна реализовываться на базе систем управления базами данных, средств защиты информации, антивирусных средств защиты информации.

Для осуществления разграничения доступа к информационным ресурсам при межсетевом взаимодействии должно применяться межсетевое экранирование, которое реализуется программными и/или программно-аппаратными межсетевыми экранами (МЭ). Межсетевой экран должен устанавливаться между защищаемой сетью, называемой внутренней, и внешней сетью. Межсетевой экран должен входить в состав защищаемой сети. При его настройке отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю и наоборот.

Подсистема анализа защищенности должна реализовываться на основе использования средств тестирования (анализа защищенности) и контроля (аудита) безопасности информации.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе назначается структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных в информационных системах персональных данных.

Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, должны допускаться к соответствующим персональным данным на основании утвержденных Перечней должностных лиц, допущенных к работе с персональными данными.

Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в утвержденных Перечнях должностных лиц, а также факты предоставления персональных данных по этим запросам должны регистрироваться автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) Учреждения или уполномоченными лицами.

При обнаружении нарушений порядка предоставления персональных данных Учреждения уполномоченные лица должны незамедлительно приостановить предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

При хранении материальных носителей информации с персональными данными (или другой конфиденциальной информацией) должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются отдельно.

Приложение № 2
к Положению по организации и
проведению работ по обеспечению
безопасности персональных данных
при их обработке в информационных
системах персональных данных
ГАУЗ «КЭД»

Описание локально-вычислительной сети (ЛВС) ГАУЗ «КЭД»:

1. Количество узлов, обрабатывающих персональные данные – 51.
2. Топология – звезда, тип – Ethernet 100Base–TX.
3. Участники сети являются источниками и потребителями информации.
4. Сеть использует стек протоколов TCP/IP.
5. Телекоммуникационные каналы предоставляются согласно Договору с провайдером ГИСТ РТ.
6. Скоростные характеристики: ЛВС – 100 Мбит/с; Интернет – 100 Мбит/с.
7. Администрирование и перечень работ определяются Администратором информационной безопасности Учреждения.
8. Участники сети, которым необходим доступ в Интернет для выполнения служебных обязанностей, допускаются с разрешения Главного врача Учреждения и имеют доступ в глобальную сеть в соответствии с разрешенными полномочиями.
9. Внесение изменений в телекоммуникационную схему ЛВС производится работниками Учреждения (или сторонней организацией по договору или контракту).

Приложение № 3
к Положению по организации и
проведению работ по обеспечению
безопасности персональных данных
при их обработке в информационных
системах персональных данных ГАУЗ
«КЭД»

Описание состава технических средств ГАУЗ «КЭД», участвующих в обработке персональных данных:

№ п/п	Технические средства	Количество	Назначение	Приме-чание
1.	Серверы	2 шт.	хранение баз данных, обработка данных ИСПДн, терминальный доступ, предоставление доступа к сетям общего пользования Интернет	
2.	Рабочие станции	49 шт.	обработка информации	
3.	Принтеры	20 шт.	распечатка документов	

№ п/п	Технические средства	Количество	Назначение	Приме-чание
4.	МФУ	8 шт.	сканирование, распечатка, тиражирование документов	
5.	Коммутаторы	1 шт.	коммутация сети	
6.	Маршрутизаторы	1 шт.	маршрутизация сети	
7.	Модем	1 шт.	обеспечение доступа к глобальной сети	

Пояснительная записка

1. Ввод в эксплуатацию, ремонт ТС, подключение ТС к сети осуществляется работниками Учреждения (или сторонней организацией по договору или контракту).

2. Оценка полноты переданного представителями фирмы-производителя, разработчика, продавца эксплуатационной документации на ТС осуществляется работниками Учреждения (или сторонней организацией по договору или контракту).

3. ТС проверяется работниками Учреждения (или сторонней организацией по договору или контракту).

4. На этапах установки и настройки, обеспечением безопасности информации занимается Администратор информационной безопасности. На этапах эксплуатации за обеспечение безопасности отвечают пользователи ТС.

Приложение № 4
к Положению по организации и
проведению работ по обеспечению
безопасности персональных данных
при их обработке в информационных
системах персональных данных ГАУЗ
«КЭД»

Сведения о программном обеспечении ГАУЗ «КЭД», установленном на серверах и рабочих станциях, участвующих в обработке персональных данных

№ п/п	Программное обеспечение	Производитель, страна	Назначение	Кто устанавливал программное обеспечение	Кто сопровождает программное обеспечение	Приме-чание
1.	Microsoft Windows 7 Professional SP1	Microsoft, США	Операционная система	Работники Учреждения	Работники Учреждения	
2.	Microsoft Office 2013	Microsoft, США	Офисный пакет приложений для работы с документами	Работники Учреждения	Работники Учреждения	
3.	Microsoft Office 2016	Microsoft, США	Офисный пакет приложений для работы с документами	Работники Учреждения	Работники Учреждения	

№ п/п	Программное обеспечение	Производитель, страна	Назначение	Кто устанавливал программное обеспечение	Кто сопровождает программное обеспечение	Приме-чание
4.	Антивирус Kaspersky Endpoint Security 10	ЗАО Лаборатория Касперского, Россия	Антивирусная программа	Работники Учреждения	Работники Учреждения	
5.	АС «Поликлиника»	ООО «Компит», г. Казань	Информационная система персональных данных			
6.	1С: Предприятие	ООО «1С», г. Москва	Информационная система персональных данных			
7.	АС «Кадры»	ООО «Компит», г. Казань	Информационная система персональных данных			
8.	Перечень льготных профессий	ПФР	Информационная система персональных данных			

Пояснительная записка

1. Оценка полноты переданного представителями фирмы-производителя, разработчика, продавца эксплуатационной документации на ПО производится Администратором информационной безопасности Учреждения.

2. Настройка ПО производится работниками Учреждения (или сторонней организацией по договору или контракту).

3. При появлении новых версий ПО, изменения в ПО вносятся работниками Учреждения (или сторонней организацией по договору или контракту).

4. Изменения в ПО могут вносить только работники Учреждения.

Приложение № 5
к Положению по организации и
проведению работ по обеспечению
безопасности персональных данных
при их обработке в информационных
системах персональных данных ГАУЗ
«КЭД»

Сведения о программно-технических средствах защиты ГАУЗ «КЭД», установленных на серверах и рабочих станциях, участвующих в обработке персональных данных

№ п/п	Средства защиты информации	Сертификат безопасности информации	Разработчик СЗИ	Кто устанавливал	Кто сопровождает	Приме-чание
1.	Microsoft Windows 7 Professional SP1	нет	Microsoft, США	Работники Учреждения	Работники Учреждения	
2.	Антивирус Kaspersky Endpoint Security 10	нет	ЗАО Лаборатория Касперского, Россия	Работники Учреждения	Работники Учреждения	

№ п/п	Средства защиты информации	Сертификат безопасности информации	Разработчик СЗИ	Кто устанавливал	Кто сопровождает	Приме-чание
3.	КриптоПро CSP 3.6		ООО «КРИПТО-ПРО», г. Москва			
4.	«КриптоПро CSP» версия 4.0 (исполнение 1-Base)	Сертификат ФСБ РФ № СФ/114-3379 действителен до 15.01.2021 г.	ООО «КРИПТО-ПРО»			
5.	VipNet Client 4.0		ОАО «ИнфоТеКС»			

Пояснительная записка

1. Настройка СЗИ производится работниками Учреждения (или сторонней организацией по договору или контракту).
2. Разграничение доступа пользователей производится с помощью стандартных средств ОС.
3. Изменения в СЗИ производятся только Администратором информационной безопасности Учреждения.

Приложение № 6
к Положению по организации и
проведению работ по обеспечению
безопасности персональных данных
при их обработке в информационных
системах персональных данных
ГАУЗ «КЭД»

РЕКОМЕНДАЦИИ
по использованию программных и аппаратных средств защиты информации и обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Мероприятия по защите ПДн при их обработке в ИСПДн от несанкционированного доступа и неправомерных действий включают в себя:

- управление доступом;
- регистрацию и учет;
- обеспечение целостности;
- контроль отсутствия недекларированных возможностей;
- антивирусную защиту;
- обеспечение безопасного межсетевого взаимодействия ИСПДн;
- анализ защищенности;
- обнаружение вторжений.

Для выполнения вышеназванных требований, необходимо наличие следующих средств защиты:

- средство защиты от несанкционированного доступа;
- межсетевой экран;
- антивирус.

При выборе того или иного средства защиты основными критериями отбора являются:

- наличие сертификатов ФСТЭК, ФСБ;
- обеспечение необходимого уровня защиты;
- производительность;
- совместимость;
- простота настройки и эксплуатации;
- техническая поддержка;
- цена.