Приложение 1
Утверждено приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных областного государственного казенного учреждения здравоохранения «Иркутская областная клиническая психиатрическая больница № 1» (ГУЗ ИОКПБ №1)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГУЗ ИОКПБ №1 (далее – Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», 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», постановления 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», приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Цель разработки настоящего Положения – установление порядка организации и проведения работ по обеспечению безопасности персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн) ГУЗ ИОКПБ №1 на протяжении всего жизненного цикла ИСПДн.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В настоящем Положении используются следующие термины и их определения:

Информационная система персональных данных – 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, если иное не предусмотрено федеральным законом.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – 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.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

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

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

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Угрозы безопасности персональных данных – 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.

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.

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн, реализуемых в рамках создаваемой системы защиты персональных данных (далее – СЗПДн).

3.2. СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн, уровня защищенности ПДн, который необходимо обеспечить, и информационных технологий, используемых в информационных системах.

3.3. Безопасность ПДн при их обработке в ИСПДн обеспечивает оператор или лицо, осуществляющее обработку ПДн по поручению оператора на основании заключаемого с этим лицом договора (далее – уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность ПДн при их обработке в информационной системе.

3.4. Выбор средств защиты информации для СЗПДн осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации (далее – ФСБ России) и Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) во исполнение Федерального закона «О персональных данных».

3.5. Структура, состав и основные функции СЗПДн определяются исходя из уровня защищенности ПДн при их обработке в ИСПДн.

3.6. СЗПДн создается в три этапа:

Этап 1. Предпроектное обследование ИСПДн и разработка технического задания на создание СЗПДн.

Этап 2. Проектирование СЗПДн, закупка, установка, настройка необходимых средств защиты информации.

Этап 3. Ввод ИСПДн с СЗПДн в эксплуатацию.

3.7. Этап 1. Проведение предпроектного обследования и разработка технического задания на создание СЗПДн.

3.7.1. Назначение ответственного за организацию обработки ПДн ГУЗ ИОКПБ №1.

3.7.2. Создание комиссии по определению уровня защищенности ПДн при их обработке в ИСПДн ГУЗ ИОКПБ №1.

3.7.3. Определение целей обработки ПДн ГУЗ ИОКПБ №1.

3.7.4. Определение перечня ИСПДн ГУЗ ИОКПБ №1 и состава ПДн, обрабатываемых в ИСПДн.

3.7.5. Определение перечня обрабатываемых ГУЗ ИОКПБ №1 ПДн.

3.7.6. Определение сроков обработки и хранения ПДн, исходя из требования, что ПДн не должны храниться дольше, чем этого требуют цели обработки этих ПДн, по достижению которых ПДн подлежат уничтожению.

3.7.7. Определение перечня используемых в ИСПДн (предлагаемых к использованию в ИСПДн) общесистемных и прикладных программных средств.

3.7.8. Определение режимов обработки ПДн в ИСПДн в целом и в отдельных компонентах.

3.7.9. Назначение ответственного за обеспечение безопасности ПДн в ИСПДн (далее – Ответственный) для разработки и осуществления технических мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн. Для каждой ИСПДн может быть назначен отдельный Ответственный.

3.7.10. Назначение ответственного пользователя криптосредств, обеспечивающего функционирование и безопасность криптосредств, предназначенных для обеспечения безопасности ПДн. Утверждение перечня лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности ПДн в ИСПДн (пользователей криптосредств).

3.7.11. Определение перечня помещений, в которых размещены ИСПДн и материальные носители ПДн.

3.7.12. Определение конфигурации и топологии ИСПДн в целом и их отдельных компонент, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня и назначения.

3.7.13. Определение технических средств и систем, используемых в ИСПДн, включая условия их расположения.

3.7.14. Формирование технических паспортов ИСПДн.

3.7.15. Разработка организационно-распорядительных документов (далее – ОРД), регламентирующих процесс обработки и защиты ПДн:

– Политика в отношении обработки персональных данных;

– Инструкции (ответственного за организацию обработки ПДн, ответственного за обеспечение безопасности ПДн в ИСПДн, пользователя ИСПДн, ответственного пользователя криптосредств);

– Раздел должностных инструкций сотрудников ГУЗ ИОКПБ №1 в части обеспечения безопасности ПДн при их обработке, включая установление персональной ответственности за нарушения правил обработки ПДн.

3.7.16. Получение (при необходимости) согласия на обработку ПДн субъектом ПДн, подписание обязательства о соблюдении конфиденциальности ПДн сотрудником ГУЗ ИОКПБ №1.

3.7.17. Утверждение форм уведомлений субъектов ПДн и форм журналов, необходимых в целях обеспечения безопасности ПДн.

3.7.18. Определение уровня защищенности ПДн при их обработке в ИСПДн в соответствии с «Требованиями к защите ПДн при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 (подготовка и утверждение акта определения уровня защищенности ПДн при их обработке в ИСПДн).

3.7.19. Определение типа угроз безопасности ПДн, актуальных для информационной системы, с учетом оценки возможного вреда в соответствии с нормативными правовыми актами, принятыми во исполнение Федерального закона «О персональных данных». Определение угроз безопасности ПДн в конкретных условиях функционирования ИСПДн (разработка моделей угроз безопасности ПДн при их обработке в ИСПДн).

3.7.20. Формирование технического задания на разработку СЗПДн по результатам предпроектного обследования на основе нормативно-методических документов ФСТЭК России и ФСБ России с учетом установленного уровня защищенности ПДн при их обработке в ИСПДн.

Техническое задание на разработку СЗПДн должно содержать:

– обоснование разработки СЗПДн;

– исходные данные создаваемой (модернизируемой) ИСПДн в техническом,

программном, информационном и организационном аспектах;

– уровень защищенности ПДн при их обработке в ИСПДн;

– ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн, и приниматься в эксплуатацию ИСПДн;

– конкретизацию мероприятий и требований к СЗПДн;

– состав и содержание работ по этапам разработки и внедрения СЗПДн

– перечень предполагаемых к использованию сертифицированных средств защиты информации.

3.8. Этап 2. Проектирование СЗПДн, закупка, установка, настройка и опытная эксплуатация необходимых средств защиты информации.

3.8.1. Создание СЗПДн является необходимым условием обеспечения безопасности ПДн, в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиям к обеспечению безопасности ПДн для соответствующего уровня защищенности ПДн при их обработке в ИСПДн и/или не нейтрализуют всех угроз безопасности ПДн для данной ИСПДн.

3.8.2. Технические меры защиты ПДн предполагают использование программно-аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов ГУЗ ИОКПБ №1. Применение технических мер должно быть регламентировано нормативным актом ГУЗ ИОКПБ №1.

3.8.3. Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

3.8.4. На стадии проектирования и создания СЗПДн для ИСПДн ГУЗ ИОКПБ №1 проводятся следующие мероприятия:

– разработка технического проекта СЗПДн;

– приобретение (при необходимости), установка и настройка серийно выпускаемых технических средств обработки, передачи и хранения информации;

– разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;

– приобретение, установка и настройка сертифицированных технических, программных и программно-технических средств защиты информации, в том числе (при необходимости) средств криптографической защиты информации;

– реализация разрешительной системы доступа пользователей ИСПДн к обрабатываемой в ИСПДн информации;

– подготовка эксплуатационной документации на используемые средства защиты информации;

– корректировка (дополнение) организационно-распорядительной документации в части защиты информации.

3.9. Этап 3. Ввод ИСПДн с СЗПДн в промышленную эксплуатацию.

3.9.1. На стадии ввода в ИСПДн (СЗПДн) осуществляются:

– опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн (при необходимости);

– приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации (при необходимости);

– контроль выполнения требований (возможно проведение данного контроля в виде аттестации по требованиям безопасности ПДн).

3.9.2. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

4. ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Работы по обеспечению безопасности ПДн проводятся в соответствии с Планом мероприятий по защите персональных данных (ПРИЛОЖЕНИЕ 1). Внутренние проверки режима защиты ПДн ГУЗ ИОКПБ №1 проводятся в соответствии с Планом внутренних проверок режима защиты персональных данных (ПРИЛОЖЕНИЕ 2).

4.2. Контроль за проведением работ по обеспечению безопасности ПДн осуществляет ответственный за организацию обработки ПДн в виде методического руководства, участия в разработке требований по защите ПДн, организации работ по выявлению возможных каналов утечки информации, согласования выбора средств вычислительной техники и связи, технических и программных средств защиты, участия в оценке соответствия ИСПДн ГУЗ ИОКПБ №1 требованиям безопасности ПДн.

4.3. При необходимости к проведению работ по обеспечению безопасности ПДн могут привлекаться специализированные организации, имеющие лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

5. РЕШЕНИЕ ВОПРОСОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ДИНАМИКЕ ИЗМЕНЕНИЯ ОБСТАНОВКИ И КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ

5.1. Модернизация СЗПДн для функционирующих ИСПДн ГУЗ ИОКПБ №1 должна осуществляться в случае:

- изменения состава или структуры ИСПДн или технических особенностей ее построения (изменения состава или структуры программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);
- изменения состава угроз безопасности ПДн в ИСПДн;
- изменения уровня защищенности ПДн при их обработке в ИСПДн;
- прочих случаях, по решению оператора.

5.2. В целях определения необходимости доработки (модернизации) СЗПДн не реже одного раза в год ответственным за организацию обработки ПДн должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и уровня защищенности ПДн при их обработке в ИСПДн, соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Результаты проверки оформляются актом проверки и утверждаются руководителем ГУЗ ИОКПБ №1.

5.3. Анализ инцидентов безопасности ПДн и составление заключений в обязательном порядке должно проводиться в случае выявления следующих фактов:

- несоблюдение условий хранения носителей ПДн;
- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн;
- нарушение заданного уровня безопасности ПДн (конфиденциальность/ целостность/доступность).

ПРИЛОЖЕНИЕ 1
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГУЗ ИОКПБ №1
от 29 марта 2017 г.

Типовой план мероприятий по защите персональных данных в ГУЗ ИОКПБ №1

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
1.	Документальное регламентирование работы с ПДн	При необходимости	Разработка организационно-распорядительных документов по защите ПДн, либо внесение изменений в существующие
2.	Получение согласий субъектов ПДн (физических лиц) на обработку ПДн в случаях, когда этого требует законодательство	Постоянно	В случаях, предусмотренных Федеральным законом «О персональных данных», обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Форма согласия приведена в Приказе «Об утверждении форм документов, необходимых в целях выполнения требований законодательства в области персональных данных». Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью
3.	Пересмотр договора с третьими лицами на поручение обработки ПДн	При необходимости	В случае поручения обработки ПДн субъектов ПДн третьим лицам (например, кредитно-финансовым учреждениям) в договор включается пункт о соблюдении конфиденциальности при обработке ПДн, а также учитываются требования ч.3 ст.6 Федерального закона «О персональных данных»
4.	Ограничение доступа сотрудников к ПДн	При необходимости (при создании ИСПДн)	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствие с требованиями закона необходимо разграничить доступ сотрудников Оператора к ПДн
5.	Взаимодействие с субъектами ПДн	Постоянно	Работа с обращениями субъектов ПДн, ведение журналов учета передачи персональных данных, обращений субъектов ПДн, уведомление субъектов ПДн об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
6.	Ведение журналов учета отчуждаемых электронных носителей персональных данных, средств защиты информации	Постоянно	
7.	Повышение квалификации сотрудников в области защиты ПДн	Постоянно	Повышение квалификации сотрудников, ответственных за выполнение работ – не менее раза в три года, повышение осведомленности сотрудников – постоянно (данное обучение проводит ответственный за обеспечение безопасности ПДн в ИСПДн)
8.	Инвентаризация информационных ресурсов	Раз в полгода	Проводится с целью выявления в информационных ресурсах присутствия ПДн
9.	Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки	При необходимости	Для ПДн Оператором устанавливаются сроки обработки ПДн, которые документально подтверждаются в нормативных документах Оператора. При пересмотре сроков необходимые изменения вносятся в соответствующие документы
10.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн	При необходимости	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн производится с оформлением Акта на списание и уничтожение электронных (бумажных) носителей информации. Форма соответствующего акта приведена в Приказе «Об утверждении форм документов, необходи-мых в целях выполнения требований законо-дательства в области персональных данных»
11.	Определение уровня защищенности ПДн при их обработке в ИСПДн	При необходимости	Определение уровня защищенности ПДн при их обработке в ИСПДн осуществляется при создании ИСПДн, при изменении состава ПДн, объема обрабатываемых ПДн, субъектов ПДн
12.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости	Разрабатывается при создании системы защиты ИСПДн
13.	Аттестация (сертификация) СЗПДн или декларирование соответствия по требованиям безопасности ПДн	При необходимости	Проводится совместно с лицензиатами ФСТЭК
14.	Эксплуатация ИСПДн и контроль безопасности ПДн	Постоянно	
15.	Понижение требований по защите ПДн путем сегментирования ИСПДн, отключения от сетей общего пользования, обеспечения обмена между ИСПДн с помощью сменных носителей, создания автономных ИСПДн на выделенных АРМ и прочих доступных мер	При необходимости	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствии с требованиями закона

ПРИЛОЖЕНИЕ 2
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГУЗ ИОКПБ №1
от 29 марта 2017 г.

План внутренних проверок режима защиты персональных данных в ГУЗ ИОКПБ №1

№	Мероприятие	Периодичность	Дата, подпись исполнителя
1.	Контроль соблюдения правил обработки ПДн	Ежемесячно	
2.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн	Ежегодно	
3.	Контроль соблюдения режима парольной защиты	Ежемесячно	
4.	Контроль выполнения антивирусной защиты	Еженедельно	
5.	Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	
6.	Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	
7.	Контроль за обеспечением резервного копирования	Ежемесячно	
8.	Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	
9.	Поддержание в актуальном состоянии нормативно-организационных документов	Ежеквартально	
10.	Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями (при наличии)	Ежемесячно	
11.	Тестирование всех функций СЗИ НСД с помощью специальных программных средств	Ежегодно	

Приложение 2
Утвержден приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ ГУЗ ИОКПБ №1

Наименование информационной системы (ИС)	**Тип ИС[1]**	**Уровень защищенности ПД**

[1] Типы ИС: ИСПДн - ИС персональных данных, ГИС – государственная ИС.

Приложение 3
Утвержден приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ПЕРЕЧЕНЬ ОБЩЕДОСТУПНЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ГУЗ ИОКПБ №1

1. Фамилия.
2. Имя.
3. Отчество.
4. Должность.
5. Образование, данные о повышении квалификации.
6. Контактная информация: служебный номер телефона, служебный адрес электронной почты.

Приложение 4
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ИНСТРУКЦИЯ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГУЗ ИОКПБ №1

Настоящая инструкция определяет общие функции, права и обязанности администратора информационной безопасности по вопросам обеспечения безопасности информации при подготовке и обработки защищаемой информации на автоматизированных рабочих станциях, входящих в состав информационных систем ГУЗ ИОКПБ №1.

Настоящая Инструкция разработана на основании действующих нормативных документов по защите информации в ГУЗ ИОКПБ №1.

1.Общие положения

1.1. Администратор информационной безопасности (далее – Администратор ИБ) назначается приказом главного врача ГУЗ ИОКПБ №1.

1.2. Администратор ИБ обеспечивает правильность использования и нормальное функционирование установленных средств защиты в ГУЗ ИОКПБ №1.

1.3. В своей деятельности администратор информационной безопасности руководствуется действующим законодательством Российской Федерации, эксплуатационной и технической документацией к средствам защиты информации, а также документацией ГУЗ ИОКПБ №1 в области обеспечения защиты информационных систем.

2.Основные функции администратора ИБ

1.4. Основные функции администратора:

– контроль за выполнением требований действующих нормативных документов по вопросам обеспечения режима конфиденциальности, при проведении работ в информационных системах (далее - ИС) ГУЗ ИОКПБ №1;

– участие в работе комиссии по пересмотру Перечня сведений, подлежащих защите;

– участие в проектировании, приемке, сдаче в промышленную эксплуатацию программных средств в информационных системах ГУЗ ИОКПБ №1 (в части требований к средствам защиты информации);

– контроль за соблюдением правил безопасной эксплуатации информационных систем ГУЗ ИОКПБ №1;

– участие в разработке и определении порядка учета, хранения и обращения с защищаемой информацией (документами и носителями информации);

– работа с учетными записями пользователей ИС ГУЗ ИОКПБ №1 (удаление, регистрация новых пользователей), их правильная настройка и разграничение прав доступа пользователей к защищаемым ресурсам информационных систем согласно разрешительной системе доступа;

– настройка и сопровождение в процессе эксплуатации подсистемы доступа ИС ГУЗ ИОКПБ №1;

– своевременная корректировка разрешительной системы доступа:

- изменение списка постоянных пользователей ИС (ввод или удаление пользователя из ИС);
- изменение прав доступа к защищаемым программным ресурсам или портам ввода-вывода ИС.

– корректировка разрешительной системы доступа осуществляется на основании служебной записки пользователя, согласованной с ответственным за обеспечение безопасности персональных данных;

– контроль доступа пользователей к работе на рабочие станции (в соответствии со списком лиц, которым необходим доступ к защищаемой информации, обрабатываемой в ИС ГУЗ ИОКПБ №1, для выполнения служебных (трудовых) обязанностей), выдача внешних носителей информации и соблюдения пользователями требований нормативных и руководящих документов (в том числе путем просмотра системного журнала);

– контроль за ежеквартальным проведением пользователями ИС смены их личных паролей для доступа к рабочим станциям;

– настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе на рабочих станциях, в том числе и в части периодического контроля за печатью файлов пользователей на принтере и соблюдением установленных правил и параметров регистрации и учета документов, бумажных и машинных носителей информации;

– сопровождение подсистемы обеспечения целостности информации на рабочих станциях:

✓ периодический контроль за отсутствием на жестком магнитном диске рабочей станции остаточной информации по окончании работы пользователей;

✓ контроль за соблюдением пользователями инструкции по организации антивирусной защиты в информационных системах ГУЗ ИОКПБ №1. Программирование, выдача и учет выдачи пользователям электронных ключей от СЗИ НСД (при их наличии).

– контроль за наличием и целостностью пломб (печатей, специальных защитных знаков) на корпусе рабочих станций и устройств.

– контроль за вскрытием и ремонтом (модернизацией) рабочих станций, недопущением доступа посторонних лиц к конфиденциальной информации во время вскрытия, ремонта, модернизации рабочих станций или устройств, последующим опечатыванием рабочих станций (устройств), составлением соответствующих актов.

– контроль срока действия сертификатов соответствия ФСТЭК России и ФСБ России на средства защиты информации, установленных в ГУЗ ИОКПБ №1.

– сопровождение подсистемы защиты информации от утечки за счет ПЭМИН, контроль соблюдения требований по размещению и использованию технических средств и систем, указанных в Предписании на эксплуатацию;

– оценивать возможность и последствия внесения изменений в состав ИС ГУЗ ИОКПБ №1, с учетом требований по защите информации, подготавливать свои предложения;

– контролировать физическую сохранность средств и оборудования ИС ГУЗ ИОКПБ №1;

– своевременно анализировать журналы учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;

– периодически предоставлять руководителю ГУЗ ИОКПБ №1 отчет о состоянии защиты ИС ГУЗ ИОКПБ №1 и о нештатных ситуациях и допущенных пользователями нарушений установленных требований по защите информации.

2. Права и обязанности администратора ИБ

2.1. Администратор ИБ имеет право:

– участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

– на организацию проведения работ по выявлению возможных каналов нарушения информационной безопасности при эксплуатации ИС и принятие своевременных мер по их перекрытию;

– на организацию контроля за выполнением специальных требований по размещению технических средств ИС, прокладке кабельных трасс и инженерных систем, за организацией резервного дублирования и архивирования информации, а также созданием и использованием эталонных копий программного обеспечения в части обеспечения безопасности информации и процессов ее обработки;

– на определение и пересмотр порядка установки и модернизации аппаратных и программных средств ИС ГУЗ ИОКПБ №1 в части обеспечения безопасности информации и процессов ее обработки;

– на определение и пересмотр порядка проектирования, разработки, отладки, проверки, внедрения и использования программного обеспечения в части обеспечения безопасности информации и процессов ее обработки.

– требовать от пользователей прекращения обработки информации в ИС в случае:

- ✓ нарушения установленного порядка работ;
- ✓ нарушения работоспособности средств и систем защиты информации или окончания срока действия сертификатов соответствия ФСБ России или ФСТЭК России;
- ✓ получения информации о возможном проведении технической разведки в отношении ИС;

– блокировать учетные записи пользователей, осуществивших несанкционированный доступ к защищаемым ресурсам;

– участвовать в любых проверках в ИС ГУЗ ИОКПБ №1;

– запрещать устанавливать на серверах и рабочих станциях нештатное программное и аппаратное обеспечение;

– осуществлять контроль за процессом резервирования и дублирования важных ресурсов ИС ГУЗ ИОКПБ №1;

– участвовать в процессе приема-передачи новых программных средств;

– уточнять в установленном порядке обязанности пользователей ИС ГУЗ ИОКПБ №1 по поддержанию уровня защиты;

– вносить предложения по совершенствованию уровня защиты ИС ГУЗ ИОКПБ №1ы;

– запрещать и немедленно блокировать попытки изменения программно-аппаратной среды ИС ГУЗ ИОКПБ №1 без согласования порядка ввода новых (отремонтированных) технических и программных средств и средств защиты информации;

– запрещать и немедленно блокировать применение пользователям ИС ГУЗ ИОКПБ №1 программ, с помощью которых возможны факты несанкционированного доступа к ресурсам ИС ГУЗ ИОКПБ №1;

– незамедлительно докладывать руководителю ГУЗ ИОКПБ №1 обо всех попытках нарушения защиты ИС ГУЗ ИОКПБ №1;

– анализировать состояние защиты ИС ГУЗ ИОКПБ №1 и ее отдельных подсистем;

– контролировать состояние средств и систем защиты информации и их параметры и критерии;

– контролировать правильность применения пользователями средств защиты информации;

– оказывать помощь пользователям в части применения средств защиты;

– не допускать установку, использование, хранение и размножение в ИС ГУЗ ИОКПБ №1 программных средств, не связанных с выполнением функциональных задач;

– осуществлять контроль за соблюдением установленных правил и параметров регистрации и учета бумажных носителей информации;

– контролировать установленный порядок и правила антивирусной защиты информации;

– контролировать отсутствие на машинных носителях остаточной информации по окончании работы;

– не допускать к работе на рабочих станциях ИС ГУЗ ИОКПБ №1 посторонних лиц.

2.2. Администратор информационной безопасности обязан:

– знать в совершенстве применяемые информационные технологии;

– участвовать в работе по определению необходимых мер защиты при проектировании программных средств автоматизации решения прикладных задач, по оценке качества реализации необходимых защитных механизмов в ИС при испытаниях и внедрении данного программного обеспечения (в части обеспечения безопасности информации и процессов ее обработки);

– участвовать в контрольных и тестовых испытаниях и проверках ИС ГУЗ ИОКПБ №1;

– обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных функций;

– в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

– проводить инструктаж пользователей по правилам работы на рабочих станциях ИС ГУЗ ИОКПБ №1 и по изучению руководящих документов по вопросам обеспечения безопасности информации;

– знать права доступа пользователей по обработке, хранению и передаче защищаемой информации;

– докладывать руководителю ГУЗ ИОКПБ №1 о неправомерных действиях пользователя, приводящих к нарушению требований по защите информации;

– вносить изменения в документацию ГУЗ ИОКПБ №1 в соответствии с требованиями нормативных документов в части, касающейся СЗИ;

– постоянно проводить работу по выявлению возможных каналов утечки конфиденциальных сведений при эксплуатации ИС и несанкционированного вмешательства в процесс ее функционирования, вести их учёт, принимать меры к их устранению;

– осуществлять не реже одного раза в неделю обновление антивирусных баз на рабочих станциях в ИС ГУЗ ИОКПБ №1;

– контролировать целостность (неизменность, сохранность) программного обеспечения, разрешительной системы доступа, а при обнаружении фактов изменения проверяемых параметров немедленно докладывать по подчинённости;

– вводить полномочия работников в разрешительную систему доступа, обеспечивать их своевременную корректировку;

– контролировать исполнение порядка учета, хранения, использования и уничтожения внешних носителей конфиденциальной информации;

– контролировать выполнение установленных правил создания, хранения и использования эталонных копий программных средств, соблюдение порядка формирования и использования информационных массивов и баз данных, резервного и архивного копирования данных (Приложение1 к настоящей инструкции);

– регистрировать факты выдачи внешних носителей в журнале учета, хранения и выдачи машинных носителей или журнале выдачи носителей с ключевой информацией соответственно.

– требовать от пользователей прекращения обработки защищаемой информации при появлении информации о возможном проведении технической разведки в отношении ИС ГУЗ ИОКПБ №1.

– заблокировать учетные записи пользователей в случае окончания срока действия сертификата соответствия ФСТЭК России, ФСБ России на любое СЗИ, из используемых в ИС ГУЗ ИОКПБ №1, до момента его продления. В случае не продления сертификата соответствия ФСТЭК России на СЗИ он обязан поставить в известность орган по аттестации, проводивший аттестацию ИС ГУЗ ИОКПБ №1, для принятия совместного решения.

– производить периодическое тестирование всех реализованных программно-техническими средствами функций и требований по обеспечению информационной безопасности;

– координировать действия должностных лиц по своевременному восстановлению процесса обработки данных в кризисных (аварийных) ситуациях;

– участвовать в расследовании причин возникновения серьезных кризисных ситуаций;

– периодически контролировать правильность ведения журналов учета нештатных ситуаций;

2.3. При выявлении факта несанкционированного доступа администратор ИБ обязан:

– блокировать доступ к конфиденциальной информации;

– проанализировать характер несанкционированного доступа

– доложить заместителю главного врача по ГО и МР ГУЗ ИОКПБ №1 служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

– принять меры к защите от несанкционированного доступа;

– по решению руководителя ГУЗ ИОКПБ №1 возобновить работу.

o Администратору информационной безопасности запрещается:

– производить действия по настройке параметров средств защиты информации;

– устанавливать срок действия учетной записи пользователя более 1 (одного) года; по истечении указанного срока в соответствии с разрешительной системой доступа производится продление действия учетной записи либо определение прав на такое продление;

– производить установку средств криптографической защиты информации;

– самостоятельно фиксировать учетные данные пользователя (пароли, идентификаторы, ключи и др.) на твердых носителях, а также сообщать их кому бы то ни было, кроме самого пользователя.

2.4. При возникновении ситуаций, не описываемых руководящими документами, решение принимает администратор ИБ, руководствуясь Положением по организации и

проведению работ по обеспечению безопасности защищаемых данных при их обработке в информационных системах ГУЗ ИОКПБ №1 и действующим законодательством РФ.

2.5. Ответственность за сохранность конфиденциальной информации несет администратор информационной безопасности, действия которых фиксируются в протоколах аудита.

2.6. Администратор информационной безопасности несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования этих учетных записей.

2.7. При нарушениях администратором информационной безопасности правил, связанных с информационной безопасностью, он несет ответственность, установленную действующим законодательством Российской Федерации.

Приложение1
к инструкции администратора
информационной безопасности в
информационных системах
ГУЗ ИОКПБ №1

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах ГУЗ ИОКПБ №1

1. Общие положения

1.1. Настоящий порядок резервирования и восстановления работоспособности технических средств (ТС) и программного обеспечения (ПО), баз данных и средств защиты информации (СЗИ) разработан с целью обеспечения возможности незамедлительного восстановления защищаемых данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.2. Данный документ:

- определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационных систем ГУЗ ИОКПБ №1, в том числе информационных систем персональных данных ГУЗ ИОКПБ №1;
- предназначен для исполнения сотрудником, в обязанности которого входит техническое обслуживание информационных систем ГУЗ ИОКПБ №1 (далее – администратор), а так же сотрудников ГУЗ ИОКПБ №1, участвующих в обработке защищаемых данных (ЗД) в ИС ГУЗ ИОКПБ №1 (далее – пользователи);
- описывает действия администратора и пользователей по обеспечению резервного копирования и восстановления ЗД, обрабатываемых в информационных системах ГУЗ ИОКПБ №1.

1.3. Носители информации, используемые для резервирования защищаемой информации ГУЗ ИОКПБ №1 (в том числе и персональных данных), подлежат защите в той же степени, что и резервируемая информация.

1.4. Контроль за исполнением настоящего порядка осуществляет администратор информационной безопасности и сотрудник, ответственный за обеспечение безопасности персональных данных в ГУЗ ИОКПБ №1.

2. Назначение и область действия

2.1. Резервируемой информацией следует считать любые защищаемые данные в электронном виде. Резервируемая информация разделяется по способу обработки (по способу хранения) на две категории:

- обработка (хранение) в базе данных;
- любом другом виде.

2.2. Резервному копированию подлежат все информационные ресурсы ГУЗ ИОКПБ №1, содержащие защищаемую информацию, а именно:

- файлы баз данных;
- электронные документы;
- файлы сообщений электронной почты;

- отсканированные и хранящиеся в ИС ГУЗ ИОКПБ №1 изображения документов и фотографии субъектов.

2.3. Резервному копированию могут так же подвергаться:

- системное и прикладное программное обеспечение ИС ГУЗ ИОКПБ №1;
- средства защиты информации.

3. Порядок резервирования

3.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых защищаемых данных - не реже одного раза в месяц;
- для технологической информации - не реже раза в два месяца;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС ГУЗ ИОКПБ №1 - не реже раза в квартал, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.2. Резервирование защищаемых информационных ресурсов ИС ГУЗ ИОКПБ №1, не содержащих персональные данные, выполняется администратором информационной безопасности.

3.3. Резервирование информационных ресурсов ИС ГУЗ ИОКПБ №1, содержащих персональные данные, выполняется ответственным за обеспечение безопасности персональных данных в ИСПДн ГУЗ ИОКПБ №1.

3.4. Определяется 2 вида резервирования данных:

- полное резервирование данных – резервное копирование всех защищаемых данных, хранящихся в ИС ГУЗ ИОКПБ №1;
- неполное резервирование данных – резервное копирование части защищаемых данных, хранящихся в ИС ГУЗ ИОКПБ №1.

3.5. Целью неполного резервирования является сохранение изменений в ИС ГУЗ ИОКПБ №1 с момента полного резервирования защищаемых данных.

3.6. Резервирование ЗД осуществляется в автоматическом режиме на локальном дисковом массиве сервера.

3.7. Резервное копирование баз данных выполняется:

- в конце рабочего дня ответственным специалистом на учтенный съемный носитель информации, если в базу данных были внесены изменения;
- ежедневно в конце рабочего дня в автоматическом режиме на локальный диск сервера.

3.8. Восстановление файлов ИС ГУЗ ИОКПБ №1 производится путем разархивирования файлов базы данных в исходный каталог.

3.9. Необходимо регулярно периодичностью один раз в квартал создавать резервные копии путем копирования информации на КОД или любой другой зарегистрированный отчуждаемый носитель информации.

3.10. Периодичность проведения работ по резервированию данных определяется ответственным за обеспечение безопасности персональных данных совместно с администратором информационной безопасности с учётом специфики работы ИС ГУЗ ИОКПБ №1, но не менее 1 раза в квартал для полного резервирования и 1 раза в месяц для неполного резервирования.

3.11. В случаях, когда защищаемые ресурсы хранятся на компьютерах пользователей локально, допустимо перекладывать ответственность за проведение неполного резервирования данных на пользователей ИС ГУЗ ИОКПБ №1.

3.12. События резервирования защищаемых данных фиксируются в Журнале резервирования информационных ресурсов ИС ГУЗ ИОКПБ №1. В журнале указывается: дата, вид резервирования, наименование резервируемого информационного ресурса, количество и общий размер файлов, серийный номер носителя информации, ответственное лицо.

3.13. Администратор ИС ГУЗ ИОКПБ №1 использует средства резервного копирования ИС для резервирования данных на отчуждаемый носитель. В случаях, когда резервирование данных средствами ИС не представляется возможным, администратор ИС по согласованию с ответственным за обеспечение безопасности персональных данных ГУЗ ИОКПБ №1 и администратором информационной безопасности может использовать средство резервного копирования, не входящее в состав ИС ГУЗ ИОКПБ №1.

3.14. Резервное копирование с использованием незащищённых каналов связи общего пользования не допустимо.

3.15. Резервное копирование по локальной сети на устройство, находящееся вне ИС, не допустимо.

3.16. Администратор не имеет право ознакамливаться с резервируемыми защищаемыми данными. Факт ознакомления администратора с резервируемыми защищаемыми данными может быть расценён как превышение служебных полномочий в соответствии с Трудовым Кодексом Российской Федерации и Кодексом об Административных Правонарушениях Российской Федерации.

3.17. При резервировании защищаемых данных не допускается хранение на одном носителе резервных копий ЗД, извлечённых из различных ИС ГУЗ ИОКПБ №1. Для осуществления резервирования защищаемых данных различных ИС, для каждой ИС должен быть предусмотрен отдельный носитель информации.

3.18. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

3.19. Носители должны храниться не менее года, для возможности восстановления данных.

3.20. В случае удаления ЗД субъекта из ИС ГУЗ ИОКПБ №1 должна быть так же удалена резервная копия этих данных.

4. Порядок хранения резервных копий

4.1. Хранение резервных копий ЗД должно исключать любой несанкционированный доступ посторонних лиц к носителям информации.

4.2. Хранение носителей резервных копий защищаемой информации должно быть организовано в сейфе или несгораемом, металлических шкафу с устройством опечатывания у администратора информационной безопасности и/или у сотрудника, ответственного за обеспечение безопасности персональных данных.

4.3. Доступ к местам хранения резервных копий должен быть предоставлен только администратору информационной безопасности и ответственному за обеспечение безопасности персональных.

4.4. На носителе информации, содержащем резервные копии ЗД, не должна храниться посторонняя информация.

5. Порядок восстановления информации после сбоя

5.1. При искажении, модификации, блокировании, удалении ЗД необходимо руководствоваться следующим порядком восстановления.

– в случае возникновения инцидента информационной безопасности, связанного с ЗД, следует незамедлительно сообщить об этом администратору;

– ответственным за восстановление ЗД из резервных копий является администратор, руководитель подразделения, в котором произошел инцидент и/или администратор информационной безопасности;

– администратор обязан срочно уведомить администратора информационной безопасности и ответственного за обеспечение безопасности персональных данных в ГУЗ ИОКПБ №1 о факте сбоя в работе ИС ГУЗ ИОКПБ №1, повлёкшего нарушение целостности ЗД;

– администратор должен оценить причину возникновения неисправности и принять меры по устранению технических неисправностей при неполадках программного или аппаратного обеспечения компьютера, или воспользоваться резервной копией при проблемах связанных непосредственно с ЗД;

– факты восстановления ЗД должны фиксироваться в Журнале резервирования информационных ресурсов ИС ГУЗ ИОКПБ №1 (в графе «вид резервирования» указывается «полное восстановление» либо «частичное восстановление»).

Приложение 5
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ИНСТРУКЦИЯ ПО РАБОТЕ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ГУЗ ИОКПБ №1

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственным за обеспечение безопасности персональных данных (далее – Ответственный) является штатный сотрудник ГУЗ ИОКПБ №1, назначенный приказом главного врача ГУЗ ИОКПБ №1.

1.2. На время отсутствия ответственного за обеспечение безопасности персональных данных его обязанности выполняет администратор информационной безопасности, который приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

1.3. Ответственный в своей работе руководствуется настоящей инструкцией, законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных и регламентирующими документами ГУЗ ИОКПБ №1.

1.4. Ответственный отвечает за обеспечение необходимого уровня безопасности персональных данных, является уполномоченным на проведение работ по защите информации и поддержанию достигнутого уровня защиты информационных систем персональных данных (ИСПДн) и ее ресурсов на этапах эксплуатации и модернизации.

1.5. Ответственный осуществляет методическое руководство сотрудников, имеющих санкционированный доступ к персональным данным (ПДн), в вопросах обеспечения безопасности персональных данных.

1.6. Требования ответственного, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми сотрудниками, имеющими санкционированный доступ к ПДн.

1.7. Ответственный за обеспечение безопасности персональных данных является лицом, ответственным за выявление инцидентов в информационной системе и реагирование на них.

1.8. Непосредственное руководство за надлежащим выполнением ответственным своих должностных обязанностей в области организации обработки персональных данных в информационных системах ГУЗ ИОКПБ №1 осуществляется главным врачом ГУЗ ИОКПБ №1.

2. ПРАВА И ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО

2.1. Ответственный обязан:

– знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних нормативных документов ГУЗ ИОКПБ №1, регламентирующих порядок действий по защите ПДн;

– анализировать состояние защиты ИСПДн ГУЗ ИОКПБ №1;

– вести инструктаж, совместно с ответственным за организацию обработки персональных данных, сотрудников имеющих доступ к персональным данным, по всем необходимым организационно-распорядительным документам в области обработки и обеспечения безопасности персональных данных.

– контроль выполнения пользователями ИСПДн введенного режима безопасности при обработке персональных данных, в том числе, соблюдения режима конфиденциальности при обращении с персональными идентификаторами, личными ключевыми дискетами и карточками паролей, со съемными машинными носителями информации, в процессе создания машинных документов, при процедурах «лечения» администратором безопасности информации зараженных файлов;

– осуществлять взаимодействие с администратором безопасности ГУЗ ИОКПБ №1 в целях контроля состояния защищенности персональных данных в ИСПДн ГУЗ ИОКПБ №1;

– выполнение, учет и контроль изменений, вносимых:

- в списки пользователей ИСПДн;
- в перечень защищаемых информационных ресурсов ИСПДн;

– организация и проведение периодического и внеочередного контроля работы пользователей;

– участие в процедурах контроля операций по безопасному удалению личных файлов пользователя при прекращении полномочий учетной записи, по уничтожению (в установленном порядке) старых карточек паролей (при замене администратором информационной безопасности паролей пользователям) и созданию новых карточек паролей;

– контролировать наличие необходимых инструкций по эксплуатации на рабочих местах сотрудников, имеющих доступ к ИСПДн ГУЗ ИОКПБ №1;

– контролировать выполнение пользователями ИСПДн ГУЗ ИОКПБ №1 требований «Инструкции по организации парольной защиты в информационных системах ГУЗ ИОКПБ №1»;

– контролировать работу пользователей в сетях общего пользования;

– оказывать помощь пользователям ИСПДн в части применения средств защиты;

– контролировать качество и своевременность выполнения должностными лицами установленных требований по обеспечению безопасности персональных данных;

– контролировать соблюдение правил допуска сотрудников в помещения, в которых находятся компоненты ИСПДн ГУЗ ИОКПБ №1;

– не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач;

– проведение анализа воздействия изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение безопасности персональных данных;

– документальное оформление изменений в конфигурации информационной системы и системы защиты персональных данных;

– в случае отказа работоспособности технических средств и/или программного обеспечения ИСПДн, в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

– организация и участие в служебных расследованиях для выяснения причин утечки или воздействия на обрабатываемую в ИСПДн информацию, компрометации паролей с целью выяснения величины нанесенного ущерба безопасности информации и выработки новых или совершенствования принятых технических и организационных мер по защите информации от реализации угрозы в будущем;

– при возникновении необходимости, организация и участие в мероприятиях, связанных с событиями вскрытия, опечатывания, модификации состава, ремонта и т.д.

технических средств ИСПДн. Опечатывание корпусов технических средств ИСПДн. Составление актов о вскрытии и опечатывании корпусов технических средств;

– принимать участие в организации и проведении расследований по фактам нарушений в области защиты ПДн и разработке предложений по устранению недостатков и предупреждению подобного рода нарушений;

– анализ инцидентов, в том числе, определение источников и причин возникновения инцидентов, а так же оценка их последствий, принятие мер по устранению последствий инцидентов;

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

2.2. Ответственный имеет право:

– требовать от пользователей ИСПДн выполнения положений следующих инструкций по обеспечению информационной безопасности ИСПДн:

- «Инструкция по организации парольной защиты в информационных системах ГУЗ ИОКПБ №1»;
- «Инструкция пользователя информационных систем ГУЗ ИОКПБ №1»;
- «Инструкция по организации антивирусной защиты в информационных системах ГУЗ ИОКПБ №1», в части их касающейся;

- участвовать в разработке мероприятий по совершенствованию системы защиты информации в ИСПДн;

- вносить изменения в конфигурацию информационной системы и системы защиты персональных данных;

- обращаться к руководителю ГУЗ ИОКПБ №1 с мотивированным предложением по приостановке процесса обработки информации в ИСПДн или отстранению от работы пользователя ИСПДн в случаях систематического нарушения режима конфиденциальности, технологии обработки информации в ИСПДн;

- требовать от пользователей и администраторов информационной системы своевременного информирования о возникновении инцидентов в информационной системе;

- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн ГУЗ ИОКПБ №1.

3. ОТВЕТСТВЕННОСТЬ

На ответственного за обеспечение безопасности персональных данных возлагается персональная ответственность за полноту и качество выполнения своих должностных обязанностей, а также за реализацию адекватных реальным угрозам безопасности информации режимных мер по защите информации и за их своевременное применение.

Приложение 6
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ИНСТРУКЦИЯ СОТРУДНИКА ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГУЗ ИОКПБ №1

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственным за организацию обработки персональных данных (далее – Ответственный) является штатный сотрудник ГУЗ ИОКПБ №1, назначенный приказом главного врача ГУЗ ИОКПБ №1.

1.2. Ответственный в своей работе руководствуется настоящей инструкцией, законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных и регламентирующими документами ГУЗ ИОКПБ №1.

1.3. Ответственный обеспечивает соответствие организации обработки персональных данных в ИСПДн ГУЗ ИОКПБ №1 законодательству Российской Федерации.

1.4. Ответственный осуществляет методическое руководство сотрудников, имеющих санкционированный доступ к персональным данным (ПДн), в вопросах обеспечения безопасности персональных данных.

1.5. Требования ответственного, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми сотрудниками, имеющими санкционированный доступ к ПДн.

1.6. Ответственный несет персональную ответственность за качество проводимых им работ по контролю действий сотрудников, имеющих санкционированный доступ к ПДн.

1.7. Непосредственное руководство за надлежащим выполнением ответственным своих должностных обязанностей в области организации обработки персональных данных в информационных системах ГУЗ ИОКПБ №1 осуществляется главным врачом ГУЗ ИОКПБ №1.

2. ФУНКЦИИ ОТВЕТСТВЕННОГО

2.1. Ответственный должен:

– знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних нормативных документов ГУЗ ИОКПБ №1, регламентирующих порядок действий по о ПДн;

– вести инструктаж, совместно с ответственным за обеспечение безопасности персональных данных, сотрудников имеющих доступ к персональным данным, по всем необходимым организационно-распорядительным документам в области обработки и обеспечения безопасности персональных данных.

– обеспечивать эксплуатацию ИСПДн ГУЗ ИОКПБ №1 в соответствии с ее назначением;

– вести и хранить документацию на ИСПДн ГУЗ ИОКПБ №1;

– уточнять, в установленном порядке, обязанности пользователей ИСПДн по обработке ПДн;

– осуществлять контроль над выполнением Плана мероприятий по защите персональных данных;

– не допускать к работе на элементах ИСПДн посторонних лиц;

– принимать меры по реагированию, в случае возникновения внештатных и аварийных ситуаций, с целью ликвидации их последствий.

2.2. Ответственный имеет право:

2.2.1. подать прошение руководству о прохождении обучения по защите персональных данных в соответствующих учебных центрах и курсах повышения квалификации;

2.2.2. вносить руководству предложения о наказании отдельных сотрудников, имеющих санкционированный доступ к ПДн, допустивших серьезные нарушения в безопасности ПДн.

2.2.3. запрашивать и получать всю необходимую информацию от сотрудников ГУЗ ИОКПБ №1 для организации и проведения работ по вопросам обеспечения безопасности персональных данных в информационных системах ГУЗ ИОКПБ №1;

2.2.4. рассматривать предложения о привлечении к проведению работ по обеспечению защиты персональных данных информационных системах ГУЗ ИОКПБ №1 на договорной основе организаций, имеющих необходимые лицензии;

2.2.5. принимать решение о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных;

2.2.6. привлекать в установленном порядке необходимых специалистов из числа сотрудников ГУЗ ИОКПБ №1 для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных в информационных системах ГУЗ ИОКПБ №1.

Приложение 7
Утвержден приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

Перечень лиц, допущенных в помещения ГУЗ ИОКПБ №1, где установлены элементы информационных систем, обрабатывающих персональные данные

Помещение № 1 -

№ п/п	Фамилия Имя Отчество	Должность
1.		
2.		
3.		

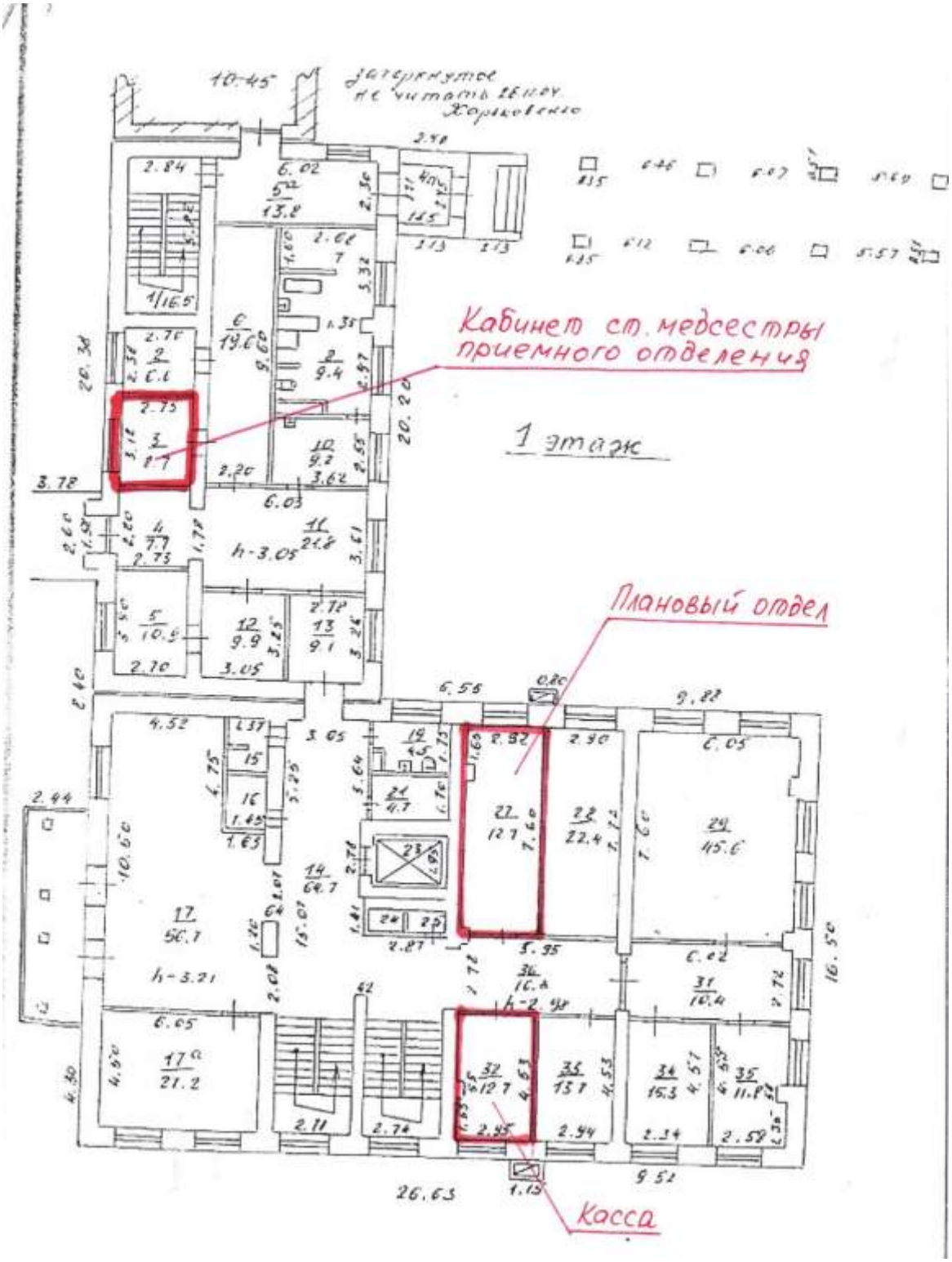
Помещение № 2 -

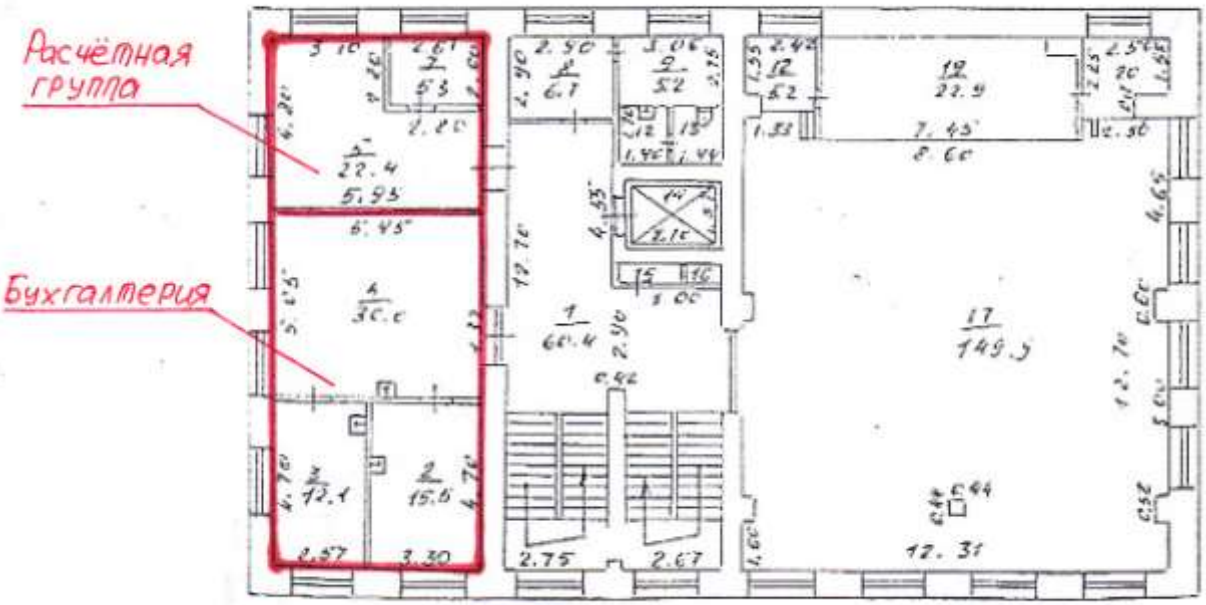
№ п/п	Фамилия Имя Отчество	Должность
4.		
5.		
6.		
7.		
8.		

Приложение 9
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

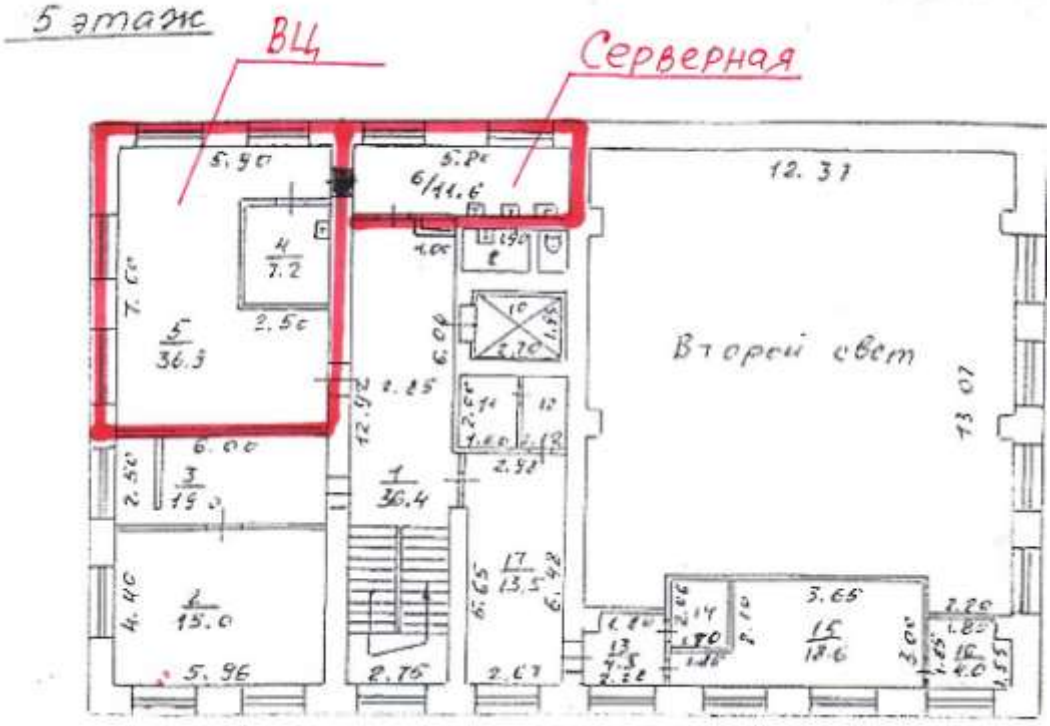
СХЕМА КОНТРОЛИРУЕМОЙ ЗОНЫ
ГУЗ ИОКПБ №1

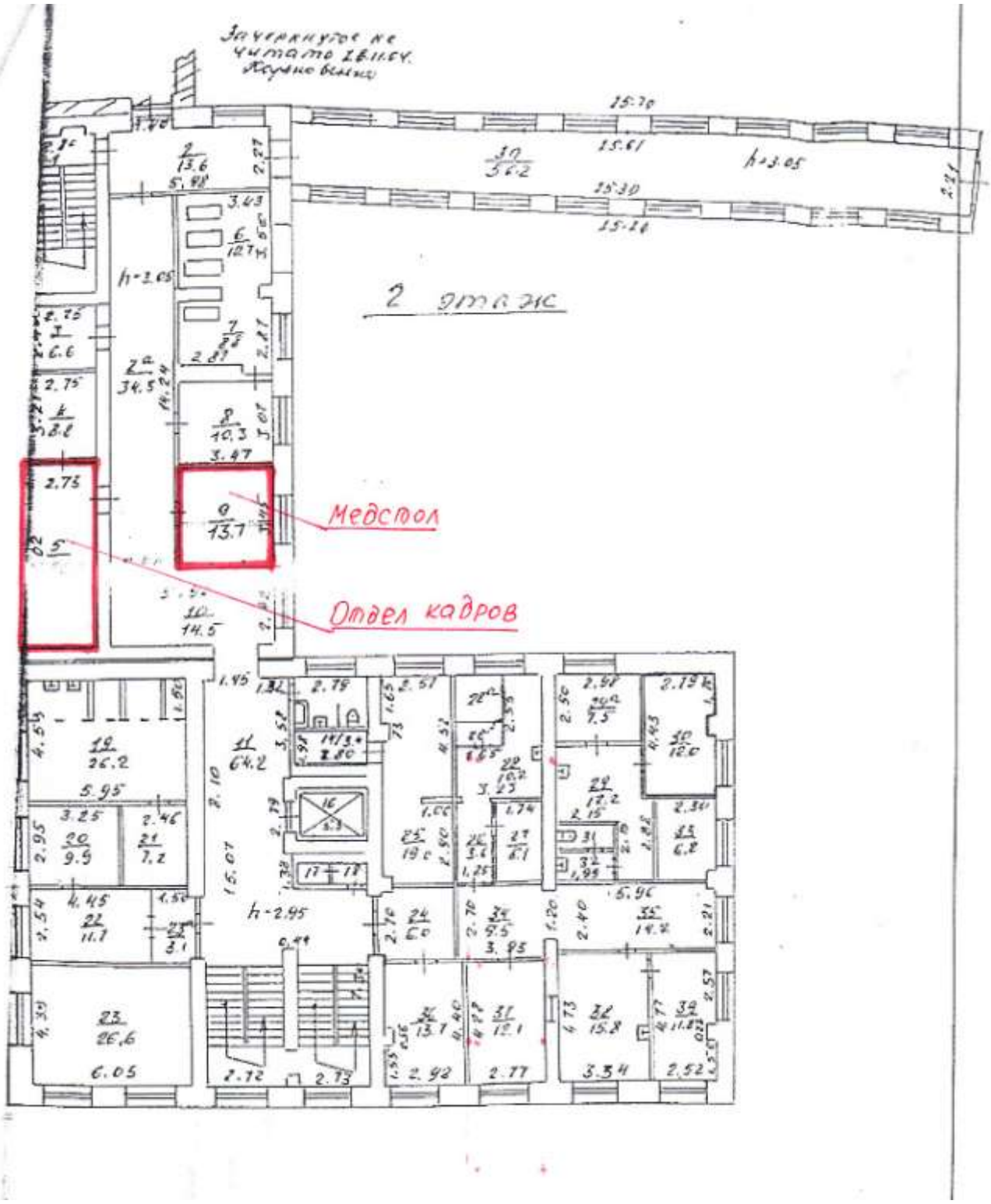
Границей контролируемой зоны являются ограждающие конструкции помещений, в которых располагаются компоненты информационных систем ГУЗ ИОКПБ №1.





5 этаж




2 этаж
Медстол
Отдел кадров

Приложение 9
Утвержден приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, РАЗРЕШЕННОГО К ИСПОЛЬЗОВАНИЮ В ИСПДн ГУЗ ИОКПБ №1

Тип программного обеспечения	Название программного обеспечения
Операционные системы	Microsoft Windows 7/8/10
Пакет офисных приложений	MS Office Standart 2007
Файловые менеджеры	FAR менеджер
Программа для работы с PDF-файлами	Adobe Reader, Foxit Reader
Программа просмотра и редактирования изображений	IrfanView
Веб-браузеры	Internet Explorer, Opera, Mozilla Firefox, Google Chrome, Yandex
Модуль для Веб-браузера	Adobe Flash Player Active
Медиаплеер	Media Player Classic, AIMP3, PotPlayer
ПО для работы с электронной подписью	КриптоПро CSP, ViPNet CSP, Континент АП
Программа проверки отчетности в ПФР	CheckPFR, ChekXML
Электронные справочники	2ГИС
Архиваторы	7-Zip
Мессенджер	Spark 2.6
Прикладное ПО	1С:Предприятие 8 Тонкий клиент, 1С:Предприятие 8, EntryCard, СБиС++ Эл. отчетность

Наименование программы	Назначение программы	Номер лицензии
Microsoft Windows 8.1 64 bit	Операционная система	номера лицензий у администратора
Microsoft Windows 7 Pro SP1 64 bit	Операционная система	номера лицензий у администратора
Microsoft Windows XP SP3	Операционная система	номера лицензий у администратора
Microsoft Office стандартный 2007	Пакет офисных приложений	номера лицензий у администратора
Adobe Flash Player Active	Модуль для Веб-браузера	свободное распространение
Windows Internet Explorer	Веб-браузер	системное программное обеспечение
Google Chrome	Веб-браузер	свободное распространение
Firefox Mozilla	Веб-браузер	свободное распространение
Opera	Веб-браузер	свободное распространение
Adobe Reader	Программа для работы с PDF файлами	свободное распространение
2ГИС	Электронный справочник с картами	свободное распространение
FAR менеджер	Файловый менеджер	свободное распространение
Double Commander	Файловый менеджер	свободное распространение
CheckPFR	Программа проверки отчетности в ПФР	свободное распространение
CheckXML	Программа проверки отчетности в ПФР	свободное распространение
Media Player Classic	Компактный медиаплеер	свободное распространение
7-zip	Архиватор для Windows	свободное распространение
USB Disk Security	программа, обеспечивающая защиту от вредоносных программ, которые пытаются проникнуть на компьютер через USB-устройства	свободное распространение
Spark	кроссплатформенное приложение, позволяющее обмениваться мгновенными сообщениями в сети Интернет по протоколу Jabber.	свободное распространение
	программное обеспечение для работы с многофункциональными устройствами и принтерами	свободное распространение

Приложение 10
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

РАЗРЕШИТЕЛЬНАЯ СИСТЕМА
ДОСТУПА К ЗАЩИЩАЕМЫМ РЕСУРСАМ ИНФОРМАЦИОННЫХ СИСТЕМ

1. ИС « »

1.1. В ИС обработка защищаемой информации осуществляется в многопользовательском режиме. Однако доступ к ИС у разных пользователей разный, матрица доступа представлена ниже.

1.2. Все пользователи ИС « » имеют собственные роли. Список ролей представлен в таблице 1.

Таблица 1

Группа (шифр)	Уровень доступа к защищаемой информации	Разрешенные действия	Сотрудники отдела

1.3. Объектами доступа в ИС « » являются:

Таблица 2

№ п/п	Объекты доступа и полномочия	Шифр
1.		
2.		
3.		
4.		

1.4. Матрица доступа пользователей к объектам доступа:

Таблица 3

Шифр объекта доступа/группа					

где:

\+ доступ предоставлен

\- доступ не предоставлен

Приложение 11
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ГУЗ ИОКПБ №1

1. Общие положения

1.1. Пользователями информационных систем (ИС) ГУЗ ИОКПБ №1, являются сотрудники, допущенные к работе в ИС ГУЗ ИОКПБ №1, в соответствии с приказом об утверждении списка лиц, которым необходим доступ к защищаемой информации, обрабатываемой в ИС ГУЗ ИОКПБ №1, для выполнения служебных (трудовых) обязанностей.

1.2. Настоящая инструкция определяет задачи, функции, обязанности, права и ответственность пользователей, допущенных к работе в ИС ГУЗ ИОКПБ №1.

1.3. Пользователем является каждый сотрудник ГУЗ ИОКПБ №1, участвующий в рамках своих функциональных обязанностей в процессах обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.4. Пользователь информационной системы персональных данных (далее по тексту - ИСПДн) осуществляет обработку персональных данных в ИСПДн.

1.5. Методическое руководство работой пользователя ИСПДн осуществляется ответственным за организацию обработки персональных данных в ИС ГУЗ ИОКПБ №1.

2. Права и обязанности пользователя

2.1. Работники, получившие доступ к защищаемой информации, обязаны хранить в тайне сведения ограниченного распространения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки защищаемой информации немедленно информировать администратора информационной безопасности и лицу ответственному за обеспечение информационной безопасности.

2.2. Защищаемая информация (в том числе персональные данные) не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению сведений ограниченного распространения.

2.3. В случае оставления занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации. В том числе: отчеты, инструкции, переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности ГУЗ ИОКПБ №1, полученные в течение срока работы.

2.4. Пользователь обязан:

– знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации;

– знать и соблюдать установленные требования по режиму обработки защищаемой информации, учету, хранению и пересылке носителей информации, обеспечению безопасности данных, а также руководящих и организационно-распорядительных документов;

– соблюдать требования парольной политики (Инструкция по организации

парольной защиты в информационных системах ГУЗ ИОКПБ №1);

– соблюдать правила при работе в сетях общего доступа и (или) международного обмена - Интернет и других (Инструкция о порядке работы при подключении к сетям общего пользования и (или) международного обмена в ГУЗ ИОКПБ №1);

– соблюдать установленную технологию обработки информации;

– руководствоваться требованиями инструкций по эксплуатации установленных средств вычислительной техники (СВТ) и средств защиты информации (СЗИ);

– экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами;

– при отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>;

– при выходе в течение рабочего дня из помещения, в котором размещается ИС, пользователь обязан:

- блокировать ввод-вывод информации на своем рабочем месте ИС в случаях кратковременного отсутствия (перерыв) или выключать СВТ ИС;
- блокировать вывод информации на монитор рабочих станций.

– немедленно ставить в известность администратора информационной безопасности:

- в случае утери носителя с персональными данными или при подозрении компрометации личных ключей и паролей;
- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах рабочих станций или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной ИС;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИС.

– обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к лицу ответственному за обеспечение информационной безопасности ИС;

– для получения консультаций по вопросам работы и настройке элементов ИС необходимо обращаться к администратору информационной безопасности.

2.5. Пользователю **ЗАПРЕЩАЕТСЯ**:

– разглашать защищаемую информацию третьим лицам;

– использовать сведения ограниченного распространения при подготовке открытых публикаций, докладов, научных работ и т.д.;

– выполнять работы с документами ограниченного распространения на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя;

– накапливать ненужные для работы персональные данные;

– передавать или принимать без расписки документы ограниченного распространения;

– оставлять на рабочих столах, в столах и незакрытых сейфах документы ограниченного распространения, а также оставлять незапертыми и не опечатанными после

окончания работы сейфы, помещения и хранилища с документами конфиденциального характера;

– осуществлять обработку защищаемой информации (в том числе персональных данных) в присутствии посторонних (не допущенных к данной информации) лиц;

– сообщать устно, письменно или иным способом (показ и т.п.) другим лицам пароли, передавать личные идентификаторы, ключевые дискеты и другие реквизиты доступа к ресурсам ИС;

– подключать к рабочим станциям нештатные устройства;

– записывать и хранить защищаемую информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.);

– несанкционированно открывать общий доступ к папкам на своей рабочей станции;

– отключать (блокировать) средства защиты информации;

– использовать компоненты программного и аппаратного обеспечения ИС подразделения в неслужебных целях;

– оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

– обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИС;

– самостоятельно вносить изменения в состав, конфигурацию и размещение ИС;

– самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения (ПО), установленного в ИС;

– самостоятельно вносить изменения в размещение, состав и настройку СЗИ ИС;

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность администратора информационной безопасности;

– привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты данных и/или администратором информационной безопасности;

– принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах, возложенных на него функций.

2.6. Пользователь имеет право:

– присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию рабочей станции, закрепленной за ним;

– обращаться к администратору информационной безопасности и/или ответственному за обеспечение безопасности персональных данных с просьбой об оказании технической и методической помощи по обеспечению безопасности обрабатываемой в ИС ГУЗ ИОКПБ №1 информации, а также по вопросам эксплуатации установленных СЗИ;

– обращаться к системному администратору (СА) с просьбой об оказании технической и методической помощи по использованию установленных программных и технических средств ИС;

– обращаться к ответственному за организацию обработки защищаемой информации по вопросам эксплуатации ИС ГУЗ ИОКПБ №1 (выполнение установленной технологии обработки информации, инструкций и других документов по обеспечению информационной безопасности объекта и защиты информации).

3. Ответственность

3.1. Пользователь несет персональную ответственность:

– за соблюдение режима безопасности защищаемых данных при их обработке и хранении в ИС ГУЗ ИОКПБ №1;

– за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИС ГУЗ ИОКПБ №1;

– за соблюдение требований инструкции, нормативных правовых актов, приказов, распоряжений и указаний, определяющих порядок организации работ по информационной безопасности при работе с защищаемой информацией.

3.2. За разглашение информации ограниченного распространения, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности

3.3. Пользователи, виновные в несоблюдении настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ «О персональных данных» и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение 12
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГУЗ ИОКПБ №1

1. Общие положения

1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах ГУЗ ИОКПБ №1, требования к содержанию паролей, а также контроль за действиями пользователей информационных систем при работе с идентификаторами и персональными паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех информационных системах ГУЗ ИОКПБ №1 и контроль за данными действиями возлагается на администратора информационной безопасности ГУЗ ИОКПБ №1 - администратора средств защиты, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

3. Контроль за действиями пользователей ИС ГУЗ ИОКПБ №1 при работе с паролями, соблюдением порядка их смены, хранения и за соответствие паролей требованиям настоящей инструкции возлагается на сотрудника, ответственного за организацию обработки персональных данных в ГУЗ ИОКПБ №1.

2. Правила формирования паролей

1. Персональные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями информационных систем самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры;
- 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 (ADMIN, SECRET, USER и т. п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- использование трех и более подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;
- личный пароль пользователь не имеет права сообщать никому;
- новый пароль не должен совпадать с одним из трех предыдущих паролей
- пользователь обязан сохранять в тайне свой личный пароль.

2. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора информационной безопасности.

3. При технологической необходимости использования учетных данных некоторых сотрудников в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т. п.) администратором информационной безопасности по запросу от

руководителей отделов ГУЗ ИОКПБ №1 предоставляется одноразовый пароль на данную учетную запись. По возвращению сотрудник обязан сменить персональный пароль на все локальное программное обеспечение.

3. Ввод пароля

1. В целях обеспечения информационной безопасности и противодействия попыткам подбора пароля в ИС ГУЗ ИОКПБ №1 определены правила ввода пароля:
   - символы вводимого пароля не отображаются на экране в явном виде;
   - учёт всех попыток (успешных и неудачных) входа в систему.

2. При первоначальном вводе или смене пароля пользователя действуют следующие правила:
   - символы вводимого пароля не должны явно отображаться на экране;
   - для подтверждения правильности ввода пароля (с учетом первого правила) - ввод пароля необходимо проводить 2 раза.

3. Ввод пароля должен осуществляться непосредственно пользователем ИС ГУЗ ИОКПБ №1 (владельцем пароля). Пользователю запрещается передавать пароль для ввода другим лицам. Передача пароля для ввода другим лицам является разглашением конфиденциальной информации и влечёт за собой ответственность согласно положениям данной Инструкции и в соответствии с действующим законодательством Российской Федерации.

4. Непосредственно перед вводом пароля для предотвращения возможности неверного ввода пользователь ИС ГУЗ ИОКПБ №1 должен убедиться в правильности языка ввода (раскладки клавиатуры), проверить, не является ли активной клавиша CAPS LOCK (если это необходимо), а также проконтролировать расположение клавиатуры (клавиатура должна располагаться таким образом, что бы исключить возможность увидеть набираемый текст посторонними).

5. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.).

4. Порядок смены личных паролей

1. Полная плановая смена паролей проводится регулярно, не реже одного раза в квартал.

2. При смене пароля администратором безопасности производится тестирование функций средств защиты информации от несанкционированного доступа путем ввода с клавиатуры заведомо ложного пароля, при наличии считывателя – предъявления стороннего идентификатора.

3. Внеплановая смена персонального пароля или удаление учетной записи пользователя информационных систем ГУЗ ИОКПБ №1 в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

4. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и т.д.) администратора информационной безопасности, сотрудника, ответственного за организацию обработки персональных данных и других сотрудников, которым для выполнения их должностных обязанностей были предоставлены полномочия по управлению парольной защитой подсистем ИС ГУЗ ИОКПБ №1.

5. Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

6. Сотрудники ГУЗ ИОКПБ №1 в течение 3-х часов после смены своих паролей должны передать их новые значения вместе с именами соответствующих учетных записей в

запечатанном конверте администратору информационной безопасности на хранение. При получении конверта с новыми паролями конверт со старыми паролями уничтожается.

7. Учетная запись пользователя, ушедшего в длительный отпуск (более 60 дней), должна блокироваться администратором информационной безопасности с момента получения письменного уведомления из отдела кадров ГУЗ ИОКПБ №1.

8. Удаление учетных записей пользователей, уволенных, переведенных в другое структурное подразделение, должно производиться администратором информационной безопасности немедленно с момента получения письменного уведомления из отдела кадров ГУЗ ИОКПБ №1.

9. Отдел кадров ГУЗ ИОКПБ №1 должен известить администратора информационной безопасности о состоявшемся приказе в течение 24 часов после увольнения, перевода сотрудника в другое структурное подразделение.

5. Хранение пароля

1. Хранение сотрудником зарегистрированных идентификаторов и значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе администратора информационной безопасности.

2. При возникновении производственной необходимости в срочном доступе к рабочей станции временно отсутствующего пользователя разрешается произвести смену пароля пользователя его непосредственным руководителем. При этом должен быть составлен акт о вскрытии конверта с паролем и о его повторном опечатывании с новым паролем.

3. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

4. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

6. Действия в случае утери и компрометации пароля

1. В случае возникновения необходимости в смене пароля в виду компрометации пользователь должен:

- немедленно сменить свой пароль;
- известить администратора информационной безопасности;
- известить сотрудника, ответственного за организацию обработки персональных данных в ГУЗ ИОКПБ №1.

2. В случае компрометации (утеря, передача парольной информации) персонального пароля пользователя информационных систем ГУЗ ИОКПБ №1 должны быть немедленно предприняты меры в соответствии с п. 4.3 или п.4.4 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Ответственность при организации парольной защиты

7.1. Владельцы паролей должны быть ознакомлены под расписку с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение информации о пароле.

7.2. Ответственность за организацию парольной защиты в ГУЗ ИОКПБ №1 возлагается на администратора информационной безопасности.

7.3. Лица, имеющие отношение к обработке персональных данных в информационных системах ГУЗ ИОКПБ №1, должны быть ознакомлены с Инструкцией под расписку.

Приложение 13
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГУЗ ИОКПБ №1

1. Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты информационных систем ГУЗ ИОКПБ №1 от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников ГУЗ ИОКПБ №1, эксплуатирующих и сопровождающих информационные системы, за выполнение требований настоящей Инструкции.

1.2. Для обеспечения информационной безопасности к использованию в ИС ГУЗ ИОКПБ №1 допускаются только лицензионные и сертифицированные ФСБ России и ФСТЭК России антивирусные средства, закупленные у официальных разработчиков (поставщиков) указанных средств.

1.3. Установка и настройка средств антивирусного контроля, контроль за состоянием антивирусной защиты в ИС ГУЗ ИОКПБ №1 осуществляется администратором информационной безопасности, в соответствии с руководствами по применению конкретных антивирусных средств.

1.4. После установки и настройки средств антивирусного контроля администратором информационной безопасности в обязательном порядке должно быть произведено тестирование системы антивирусной защиты.

1.5. Ответственность за организацию и проведение мероприятий антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.

1.6. Ответственность за ежедневный антивирусный контроль в процессе эксплуатации ИС ГУЗ ИОКПБ №1 и своевременное информирование администратора информационной безопасности в случае обнаружения действий вредоносных программ возлагается на сотрудников ГУЗ ИОКПБ №1.

2. Применение средств антивирусного контроля

2.1. Обязательному антивирусному контролю подлежат все рабочие станции (далее - РС) сотрудников ГУЗ ИОКПБ №1, а также любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.).

2.2. Антивирусный контроль рабочих станций сотрудников ГУЗ ИОКПБ №1 должен проводиться ежедневно в автоматическом режиме при начальной загрузке РС (для серверов ГУЗ ИОКПБ №1 - при перезапуске).

2.3. Настройка средств антивирусной защиты должна реализовывать следующие функции:

– непрерывный автоматический мониторинг информационного обмена в ИС с целью выявления программно-математического воздействия (далее – ПМВ);

– автоматическая проверка на наличие вредоносных программ или последствий ПМВ при импорте в ИС всех программных модулей (прикладных программ), которые могут содержать вредоносные программы, по их типовым шаблонам и с помощью эвристического анализа;

– реализация механизма автоматического блокирования обнаруженных вредоносных программ путем их удаления из программных модулей или уничтожения;

– автоматическая проверка критических областей автоматизированных рабочих мест и серверов, таких как системная память, загрузочные секторы дисков, объекты автозапуска, каталоги операционной системы «system» и «system32» при каждом запуске операционной системы;

– полная автоматическая проверка носителей информации всех автоматизированных рабочих мест и серверов не реже одного раза в неделю;

– регулярное обновление антивирусных баз и программных модулей средств антивирусной защиты. Для чего администратором информационной безопасности должен быть организован доступ к серверам обновлений разработчика антивирусного средства. В случае невозможности настроить доступ к серверам обновлений разработчика антивирусного средства, ответственному специалисту необходимо один раз в неделю осуществлять установку пакетов обновлений вирусных баз, контроль их подключения к антивирусному пакету и проверку РС на наличие вирусов;

– автоматическое документирование состояния системы антивирусной защиты ИС.

2.4. Антивирусный контроль входящей информации (в т.ч. разархивирование) должен проводиться непосредственно после получения информации на выделенном автономном компьютере. Антивирусный контроль исходящей информации должен проводиться непосредственно перед отправкой (записью на съемный носитель).

2.5. Пользователи ИС ГУЗ ИОКПБ №1 при работе со съемными носителями информации (flash-накопители, CD/DVD диски, жесткие диски USB и т.д.) обязаны перед началом работы осуществить их проверку на предмет отсутствия вредоносных программ выполнив следующие действия:

- Подключить съемный носитель информации.
- Открыть значок Рабочего стола «Мой компьютер».
- Установить курсор мыши на имя выбранного носителя.
- По правой клавише мыши открыть контекстное меню Microsoft Windows и выбрать пункт, запускающий антивирусную проверку электронного носителя информации.

2.6. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.7. Установка (изменение) системного и прикладного программного обеспечения должна осуществляться только в присутствии администратора информационной безопасности. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) системного программного обеспечения должна проводиться антивирусная проверка. В ИС ГУЗ ИОКПБ №1 запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

2.8. При возникновении подозрения на наличие в системе компьютерного вируса, (нетипичная работа программ, искажение данных, частое появление сообщений о системных ошибках и т.п.) сотрудником ГУЗ ИОКПБ №1 должен быть проведён внеочередной антивирусный контроль рабочей станции (самостоятельно или вместе с администратором информационной безопасности). Для проведения контроля должны использоваться актуальные версии антивирусных сканеров (cureit, avz и др.), запускаемых без установки в системе

2.9. В случае обнаружения при проведении антивирусной проверки наличия в системе компьютерного вируса сотрудники ГУЗ ИОКПБ №1 обязаны:

– немедленно поставить в известность администратора информационной безопасности и прекратить какие-либо действия на персональном компьютере приостановить работу;

– Поставить в известность владельца зараженных файлов.

2.10. В случае обнаружения наличия в системе компьютерного вируса необходимо:

– совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

– провести локализацию вируса в системе;

– обеспечить удаление вируса из системы;

– в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, необходимо направить зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку;

– по факту обнаружения вируса должна быть составлена служебная записка администратору информационной безопасности, в которой требуется указать предположительный источник (отправителя, владельца и т.д.) вируса, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

Пользователю ИС ГУЗ ИОКПБ №1 запрещается:

– использовать на СВТ съемные носители информации без предварительной проверки установленными средствами антивирусной защиты;

– запускать неизвестные приложения, пришедшие по электронной почте.

Пользователь обязан:

– ежедневно при начальной загрузке РС убедиться в наличии резидентного антивирусного монитора и в случае его отсутствия уведомить об этом администратора информационной безопасности;

– самостоятельно запускать внеплановую антивирусную проверку РС при получении уведомления о наличии в системе вируса, а также при возникновении подозрения на наличие вируса.

3. Ответственность

3.1. Ответственность за организацию антивирусного контроля в ГУЗ ИОКПБ №1, в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.

3.2. Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности и всех сотрудников, являющихся пользователями ИС ГУЗ ИОКПБ №1.

3.3. Периодический контроль за состоянием антивирусной защиты в ГУЗ ИОКПБ №1, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками ГУЗ ИОКПБ №1 осуществляется администратором информационной безопасности.

3.4. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора информационной безопасности.

3.5. Сотрудники ГУЗ ИОКПБ №1, нарушившие требования настоящего документа, привлекаются к ответственности в соответствии с действующим законодательством Российской Федерации.

Приложение14
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ИНСТРУКЦИЯ ПО ДЕЙСТВИЯМ ПЕРСОНАЛА ВО ВНЕШТАТНЫХ СИТУАЦИЯХ ПРИ ОБРАБОТКЕ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГУЗ ИОКПБ №1

1. Назначение и область действия

1.1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем (ИС) ГУЗ ИОКПБ №1, меры и средства поддержания непрерывности работы и восстановления работоспособности ИС ГУЗ ИОКПБ №1 после аварийных ситуаций.

1.2. Целью настоящего документа является превентивная защита элементов ИС ГУЗ ИОКПБ №1 от прерывания в случае реализации рассматриваемых угроз.

1.3. Задачей данной Инструкции является:

- определение мер защиты от прерывания;
- определение действий восстановления в случае прерывания.

1.4. Действие настоящей Инструкции распространяется на всех сотрудников ГУЗ ИОКПБ №1, имеющих доступ к ресурсам ИС ГУЗ ИОКПБ №1, а также к основным системам обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- система жизнеобеспечения;
- система обеспечения отказоустойчивости;
- система резервного копирования и хранения данных;
- система контроля физического доступа.

1.5. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

2. Порядок реагирования на аварийную ситуацию

2.1. В настоящем документе под аварийной ситуацией (инцидентом) понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИС ГУЗ ИОКПБ №1, предоставляемых пользователям ИС. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении 1 к настоящей инструкции - «Источники угроз».

2.2. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в журнале учета мероприятий по контролю обработки и защиты в информационных системах ГУЗ ИОКПБ №1.

2.3. Инцидент может возникнуть в результате преднамеренных действий злоумышленника или непреднамеренных действий пользователей, аварий, стихийных бедствий.

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники ГУЗ ИОКПБ №1 (администратор информационной безопасности, ответственный за обеспечение безопасности персональных данных, ответственный за организацию обработки персональных данных) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим

руководством. По необходимости, иерархия может быть нарушена с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.5. Уровни реагирования на инцидент. При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

– уровень 1 - незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИС ГУЗ ИОКПБ №1 и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

– уровень 2 - авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИС ГУЗ ИОКПБ №1 и средств защиты. Эти инциденты выходят за рамки ГУЗ ИОКПБ №1 ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

а) отказ элементов ИС ГУЗ ИОКПБ №1 и средств защиты из-за:

- повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;
- сбоя системы кондиционирования.

б) отсутствие администратора информационной безопасности более чем на сутки из-за:

- химического выброса в атмосферу;
- сбоев общественного транспорта;
- эпидемии;
- массового отравления персонала;
- сильного снегопада;
- торнадо;
- сильных морозов.

– уровень 3 - Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИС ГУЗ ИОКПБ №1 и средств защиты, а также к угрозе жизни пользователей ИС ГУЗ ИОКПБ №1, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИС ГУЗ ИОКПБ №1 и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

- пожар в здании;
- взрыв;
- просадка грунта с частичным обрушением здания;
- массовые беспорядки в непосредственной близости от Объекта.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

3.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

а) системы жизнеобеспечения, что включает:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

б) системы обеспечения отказоустойчивости;

в) системы резервного копирования и хранения данных;

г) системы контроля физического доступа;

д) пожарные сигнализации и системы пожаротушения;

е) системы вентиляции и кондиционирования.

3.2. Все критичные помещения ГУЗ ИОКПБ №1 (помещения, в которых размещаются элементы ИС ГУЗ ИОКПБ №1 и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.3. Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИС описан в Порядке резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ.

3.4. Ответственные за реагирование сотрудники ознакомляют всех сотрудников ГУЗ ИОКПБ №1, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу.

3.5. Должно быть проведено обучение должностных лиц ГУЗ ИОКПБ №1, имеющих доступ к ресурсам ИС ГУЗ ИОКПБ №1, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

- оказание первой медицинской помощи;
- пожаротушение;
- эвакуация людей;
- защита материальных и информационных ресурсов;
- методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;
- выключение оборудования, электричества, водоснабжения, газоснабжения.

3.6. Администратор информационной безопасности должен быть дополнительно обучен методам частичного и полного восстановления работоспособности элементов ИС ГУЗ ИОКПБ №1.

3.7. Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

3.8. Ответственность за организацию обучения должностных лиц несет руководитель отдела. Сроки и порядок их обучения согласуется с администратором информационной безопасности.

Приложение1
к инструкции по действиям персонала во внештатных ситуациях при обработке защищаемой информации в информационных системах ГУЗ ИОКПБ №1

Источники угроз

1. Технологические угрозы	
	Пожар в здании
	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
	Химический выброс в атмосферу
2. Внешние угрозы	
	Массовые беспорядки
	Сбои общественного транспорта
	Эпидемия
	Массовое отравление персонала
3. Стихийные бедствия	
	Удар молнии
	Сильный снегопад
	Сильные морозы
	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
	Затопление водой в период паводка
	Наводнение, вызванное проливным дождем
	Торнадо
	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
4. Телеком и ИТ угрозы	
	Сбой системы кондиционирования
	Сбой ИТ - систем
5. Угроза, связанная с человеческим фактором	
	Ошибка персонала, имеющего доступ к помещению, где расположено серверное оборудование
	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
6. Угрозы, связанные с внешними поставщиками	
	Отключение электроэнергии
	Сбой в работе интернет-провайдера
	Физически разрыв внешних каналов связи

Приложение15
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ИНСТРУКЦИЯ ПО ПРИЕМУ ПОД ОХРАНУ КАБИНЕТОВ ГУЗ ИОКПБ №1

1. Общие положения

1.1. Настоящая инструкция определяет порядок приема под охрану кабинетов ГУЗ ИОКПБ №1 дежурным по ГУЗ ИОКПБ №1.

1.2. В роли дежурного может выступать сторонняя охранная организация на основании заключенного договора с ГУЗ ИОКПБ №1 об оказании соответствующих услуг.

1.3. Сдачу режимных помещений (спец. помещений) под охрану, а также получение ключей и вскрытие помещений, производят сотрудники ГУЗ ИОКПБ №1 по утвержденным руководителем ГУЗ ИОКПБ №1 или руководителями подразделений спискам. Утвержденные списки с образцами подписей сотрудников передаются дежурному.

2. Порядок сдачи кабинетов ГУЗ ИОКПБ №1 под охрану

2.1. По окончании рабочего дня сотрудники ГУЗ ИОКПБ №1:

- выключают свет;
- отключают все электронные приборы и внешнее освещение;
- закрывают окна и двери кабинетов;
- сдают кабинет под роспись в Журнале приема (сдачи) под охрану кабинетов дежурному.

2.2. Дежурный, убедившись в надежности закрытия входной двери кабинетов, принимает помещение под охрану.

2.3. О приеме под охрану дежурный расписывается в журнале приема (сдачи) под охрану кабинетов с отметками о времени сдачи помещения под охрану.

2.4. При обнаружении повреждения запоров или других признаков, указывающих на возможное проникновение в помещение посторонних лиц, дежурный ставит в известность о случившемся руководителя ГУЗ ИОКПБ №1, организует охрану места происшествия до его прибытия.

3. Порядок вскрытия кабинетов ГУЗ ИОКПБ №1

3.1. Перед вскрытием кабинетов, работник:

- проверяет исправность запоров;
- в Журнале приема (сдачи) под охрану кабинетов делает отметку о дате и времени вскрытия помещения с указанием фамилии вскрывшего;
- вскрывает помещение.

3.2. При обнаружении повреждения запоров или других признаков, указывающих на возможное проникновение в помещение посторонних лиц, работник ставит в известность о случившемся главного врача ГУЗ ИОКПБ №1 и дежурного, организует охрану места происшествия до их прибытия.

3.3. Вскрытие помещения производится по акту в присутствии главного врача ГУЗ ИОКПБ №1, сотрудника, обнаружившего нарушение, и дежурного.

4. Действия в случае обнаружения пожара в кабинетах ГУЗ ИОКПБ №1

4.1. При обнаружении дыма или иных признаков возгорания в кабинетах ГУЗ ИОКПБ №1, дежурный действует согласно инструкции на случай возникновения пожара и ставит в известность о случившемся руководителя ГУЗ ИОКПБ №1.

Приложение16
Утверждено приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО РАБОТНИКА ГУЗ ИОКПБ №1, НЕПОСРЕДСТВЕННО ОСУЩЕСТВЛЯЮЩЕГО ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ, В СЛУЧАЕ РАСТОРЖЕНИЯ С НИМ СЛУЖЕБНОГО КОНТРАКТА ИЛИ ТРУДОВОГО ДОГОВОРА ПРЕКРАТИТЬ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ, СТАВШИХ ИЗВЕСТНЫМИ ЕМУ В СВЯЗИ С ИСПОЛНЕНИЕМ ДОЛЖНОСТНЫХ (СЛУЖЕБНЫХ) ОБЯЗАННОСТЕЙ

Мне,

_____,

(фамилия, имя, отчество полностью)[)]

паспорт (иной документ, удостоверяющий личность)_____

(серия, номер, кем и когда выдан)

_____

_____

известно, что в период работы в ГУЗ ИОКПБ №1 персональные данные, ставшие мне известными в связи с исполнением должностных обязанностей, относятся к категории конфиденциальной информации, имеют ограниченный доступ и разглашению не подлежат.

В случае расторжения со мной служебного контракта, освобождения меня от замещаемой должности и увольнения из ГУЗ ИОКПБ №1, прекращения (расторжения) трудового договора обязуюсь:

1. Не разглашать персональные данные, ставшие мне известными в связи с исполнением должностных обязанностей в ГУЗ ИОКПБ №1, третьей стороне без письменного согласия субъектов персональных данных, за исключением случаев, когда это требуется в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных законодательством.

2. Не использовать персональные данные, ставшие мне известными в связи с исполнением должностных обязанностей в ГУЗ ИОКПБ №1, в коммерческих целях без письменного согласия субъектов персональных данных.

3. Прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей в ГУЗ ИОКПБ №1.

4. Не копировать лично и не давать поручения копировать электронную базу данных, не допускать её копирования третьими лицами, сдать все имеющиеся электронные носители, принадлежащие ГУЗ ИОКПБ №1.

Мне разъяснены положения действующего законодательства об обеспечении сохранности персональных данных субъектов персональных данных.

Мне известно, что нарушение этих положений может повлечь дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

«____»_____20___г. _____

(подпись, расшифровка подписи)

Приложение17
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ТИПОВАЯ ФОРМА РАЗЪЯСНЕНИЯ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ ЮРИДИЧЕСКИХ ПОСЛЕДСТВИЙ ОТКАЗА ПРЕДОСТАВИТЬ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Мне,

_____,

(фамилия, имя, отчество полностью)[)]

паспорт (иной документ, удостоверяющий личность)_____

(серия, номер, кем и когда выдан)

_____

_____

разъяснены юридические последствия отказа предоставить свои персональные данные ГУЗ ИОКПБ №1.

В соответствии с Постановлением Правительства Российской Федерации от 21 марта 2012 года № 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» и «Правилами обработки персональных данных в ГУЗ ИОКПБ №1», утвержденными приказом от 29 марта 2017 г. № 121, определён перечень персональных данных, которые субъект персональных данных обязан предоставить в связи с решением вопросов в сфере деятельности, оказанием государственной услуги, реализацией права на труд, права на пенсионное обеспечение, права на медицинское страхование работников.

Я предупрежден, что в случае отказа предоставить свои персональные данные ГУЗ ИОКПБ №1 при решении вопросов в сфере деятельности, пенсионного обеспечения и медицинского страхования не могут быть реализованы в полном объёме, а служебный контракт подлежит расторжению.

«____»_____20___г. _____

(подпись, расшифровка подписи)

Юридические последствия отказа предоставить персональные данные разъяснил (а):

_____ _____ _____

(должность) (подпись) (Ф.И.О.)

Приложение 19
Утверждены приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ПРАВИЛА РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ в ГУЗ ИОКПБ №1

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей (далее - Правила) устанавливают единый порядок рассмотрения запросов субъектов персональных данных или их представителей в ГУЗ ИОКПБ №1.

2. Рассмотрение запросов субъектов персональных данных или их представителей в ГУЗ ИОКПБ №1 осуществляется в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ), настоящими Правилами и другими нормативными правовыми актами, касающимися обработки персональных данных.

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных Федеральным законом № 152-ФЗ.

4. Целью настоящих Правил является реализация прав субъекта персональных данных на получение информации, касающейся обработки его персональных данных в ГУЗ ИОКПБ №1.

5. К субъектам, персональные данные которых обрабатываются, относятся:

- граждане, находящиеся на стационарном лечении в ГУЗ ИОКПБ №1;
- граждане, находящиеся в трудовых отношениях с ГУЗ ИОКПБ №1.

II. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

6. Право субъекта персональных данных на доступ к его персональным данным:

6.1. Субъект персональных данных имеет право на получение сведений, указанных в пункте 6.7, за исключением случаев, предусмотренных пунктом 6.8. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Сведения, указанные в пункте 6.7, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6.3. Сведения, указанные в пункте 6.7, предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. В запросе указываются сведения о субъекте персональных данных или его представителе в соответствии с пунктом 9.

6.4. В случае, если сведения, указанные в пункте 6.7, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в

пункте 6.7, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодно приобретателем или поручителем по которому является субъект персональных данных.

6.5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 6.7, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 6.4, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 9, должен содержать обоснование направления повторного запроса.

6.6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 6.4 и 6.5 настоящей статьи. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

6.7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом №152-ФЗ;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

6.8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

7. Право на обжалование действий или бездействия оператора

7.1. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы, субъект персональных данных вправе

обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

7.2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

III. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ОПЕРАТОРОМ СВЕДЕНИЙ ПО ЗАПРОСУ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

8. При обращении либо при получении запроса субъекта персональных данных или его представителя, сведения должны быть предоставлены в доступной форме. Запрос регистрируется в день поступления по правилам делопроизводства.

9. Запрос субъекта персональных данных должен содержать сведения, позволяющие провести его идентификацию:

- фамилию, имя, отчество субъекта персональных данных и его представителя;
- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором;
- подпись субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

10. Оператор, при получении запроса субъекта персональных данных или его представителя, обязан сообщить в порядке статьи 14 Федерального закона № 152-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 в течении 30 (тридцати) дней с даты получения запроса.

В случае отказа в предоставлении информации о наличии персональных данных, оператор обязан дать в письменной форме мотивированный ответ со ссылкой на действующее законодательство, являющееся основанием для такого отказа. Отказ в предоставлении информации направляется в срок, не превышающий 30 (тридцать) дней со дня получения запроса субъекта персональных данных.

11. В случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор в срок, не превышающий 7(семь) рабочих дней, вносит в них необходимые изменения. О внесённых изменениях уведомляется субъект персональных данных или его представитель.

12. В случае предоставления 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 в срок, не превышающий 7(семь) рабочих дней. Об уничтоженных персональных данных уведомляется субъект персональных данных или его представитель.

13. Возможность ознакомления с персональными данными предоставляется на безвозмездной основе лицом, ответственным за обработку персональных данных.

Приложение 20
Утверждены приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, УСТАНОВЛЕННЫМ ФЕДЕРАЛЬНЫМ ЗАКОНОМ «О ПЕРСОНАЛЬНЫХ ДАННЫХ», ПРИНЯТЫМИ В СООТВЕТСТВИИ С НИМ НОРМАТИВНЫМИ ПРАВОВЫМИ АКТАМИ И ЛОКАЛЬНЫМИ АКТАМИ ГУЗ ИОКПБ №1

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами ГУЗ ИОКПБ №1 (далее – Правила) устанавливают порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГУЗ ИОКПБ №1.

2. Осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГУЗ ИОКПБ №1 осуществляется в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон №152-ФЗ), постановлением Правительства Российской Федерации от 21 марта 2012 года № 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», настоящими Правилами и другими нормативными правовыми актами, касающимися обработки персональных данных.

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных Федеральным законом № 152-ФЗ.

4. Целью осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – внутренний контроль) является обеспечение защиты персональных данных от несанкционированного доступа, неправомерного их использования или утраты, определение порядка и правил осуществления внутреннего контроля.

5. Внутренний контроль делится на текущий, плановый и внеплановый.

6. Текущий внутренний контроль осуществляется на постоянной основе ответственным за организацию обработки персональных данных в ГУЗ ИОКПБ №1 (далее – ответственный за организацию обработки) в ходе мероприятий по обработке персональных данных.
Ответственный за организацию обработки имеет право:

- запрашивать у сотрудников ГУЗ ИОКПБ №1 информацию, необходимую для реализации полномочий;

- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить главному врачу ГУЗ ИОКПБ №1 предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить главному врачу ГУЗ ИОКПБ №1 предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации о персональных данных.

7. Плановый внутренний контроль осуществляется комиссией, образуемой приказом руководителя ГУЗ ИОКПБ №1, в состав которой входят работники ГУЗ ИОКПБ №1, допущенные к обработке персональных данных.
Плановый внутренний контроль соответствия обработки персональных данных установленным требованиям в ГУЗ ИОКПБ №1 проводится на основании утвержденного руководителем ГУЗ ИОКПБ №1 плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям, разрабатываемого председателем комиссии. Периодичность плановой проверки - не реже одного раза в год.

8. Внеплановый внутренний контроль может осуществляться на основании поступившего в ГУЗ ИОКПБ №1 письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется председателем комиссии в течение 3 рабочих дней с момента поступления соответствующего заявления.
В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в её результатах.

9. При проведении внутреннего контроля ответственным за организацию обработки или комиссией должны быть полностью, объективно и всесторонне изучены:
- наличие, учет, порядок хранения и обезличивания персональных данных;
- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных;
- состояние учёта ПЭВМ и съемных носителей информации, содержащей персональные данные;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным;
- порядок проведения мероприятий и результаты по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- порядок проведения мероприятий по обеспечению целостности персональных данных.

10. В отношении персональных данных, ставших известными членам комиссии или ответственному за организацию обработки в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

11. Срок проведения плановой и внеплановой проверки не может составлять более 30 дней со дня принятия решения о её проведении.

12. Результаты внутреннего контроля оформляются в виде протокола проведения внутренней проверки (далее – протокол).

13. При выявлении в ходе внутреннего контроля нарушений ответственным за организацию обработки либо председателем комиссии в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

14. Протоколы хранятся у ответственного за организацию обработки в течение текущего года. Уничтожение протоколов проводится ответственным за организацию обработки самостоятельно в январе года, следующего за проверочным годом

15. О результатах внутреннего контроля и мерах, необходимых для устранения нарушений, руководителю ГУЗ ИОКПБ №1 докладывает ответственный за организацию обработки либо председатель комиссии.

Приложение 21
Утверждены приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ПРАВИЛА
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГУЗ ИОКПБ №1

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Правила обработки персональных данных в ГУЗ ИОКПБ №1 (далее – Правила) устанавливают единый порядок обработки персональных данных в ГУЗ ИОКПБ №1.

2. Обработка персональных данных в ГУЗ ИОКПБ №1 осуществляется в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), настоящими Правилами и другими нормативными правовыми актами, касающимися обработки персональных данных.

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных Федеральным законом № 152-ФЗ.

4. Целью настоящих Правил является обеспечение защиты персональных данных граждан 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.

5. Настоящие Правила устанавливают и определяют:
1) процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;
2) цели обработки персональных данных;
3) содержание обрабатываемых персональных данных для каждой цели обработки персональных данных;
4) категории субъектов, персональные данные которых обрабатываются;
5) сроки обработки и хранения обрабатываемых персональных данных;
6) порядок уничтожения обработанных персональных данных при достижении целей обработки или при наступлении иных законных оснований.

6. Основные условия обработки персональных данных:
6.1. Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных, а именно:

- после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных пунктами 2-7, 9-11 части 1 статьи 6 Федерального закона № 152-ФЗ;
- после направления уведомления об обработке персональных данных в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций по Иркутской области, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона №152-ФЗ.

6.2. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящими Правилами и подписывают обязательство о неразглашении информации в порядке, установленном в ГУЗ ИОКПБ №1.

II. ПРОЦЕДУРЫ, НАПРАВЛЕННЫЕ НА ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7. Меры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации:

7.1. Информационные ресурсы, содержащие персональные данные, созданные, приобретенные, накопленные в ГУЗ ИОКПБ №1, а также полученные путем иных установленных законом способов, являются собственностью ГУЗ ИОКПБ №1 и не могут быть использованы иначе, как в установленных законом случаях или с разрешения руководителя ГУЗ ИОКПБ №1.

7.2. К мерам, направленным на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных относятся:

- назначение ответственного за организацию обработки персональных данных в ГУЗ ИОКПБ №1;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с частями 1 и 2 статьи 19 Федерального закона №152-ФЗ;
- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону №152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;
- оценка вреда, который может быть причинён субъектам персональным данных в случае нарушения законодательства Российской Федерации и настоящих Правил;
- ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных и настоящими Правилами;
- запрет на обработку персональных данных лицами, не допущенными к их обработке;
- запрет на обработку персональных данных под диктовку.

7.3. Документы, определяющие политику в отношении обработки персональных данных, подлежат обязательному опубликованию на официальном сайте ГУЗ ИОКПБ №1 в течении 10 дней после их утверждения.

7.4. За разглашение информации, содержащей персональные данные, нарушение порядка обращения с документами и машинными носителями информации, содержащими такую информацию, а также за нарушение режима защиты, обработки и порядка использования этой информации, работник ГУЗ ИОКПБ №1 может быть привлечен к дисциплинарной или иной ответственности, предусмотренной действующим законодательством.

8. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации:

8.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации ГУЗ ИОКПБ №1 осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

8.2. При эксплуатации автоматизированных информационных систем необходимо соблюдать следующие требования:

- к работе допускаются только лица, назначенные соответствующим приказом;

- на персональных электронных вычислительных машинах (далее – ПЭВМ), дисках, папках и файлах, на которых обрабатываются и хранятся сведения о персональных данных, должны быть установлены пароли (идентификаторы);
- на период обработки защищаемой информации в помещении могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации;
- допуск других лиц в указанный период может осуществляться с разрешения руководителя ГУЗ ИОКПБ №1 или его заместителя, отвечающего за защиту информации в ГУЗ ИОКПБ №1.

8.3. Руководители отделов ГУЗ ИОКПБ №1, работники ГУЗ ИОКПБ №1 осуществляющие обработку персональных данных (далее - пользователи) обязаны контролировать и выполнять предусмотренные в ГУЗ ИОКПБ №1 меры по защите информации, содержащей персональные данные.

8.4. Руководители отделов ГУЗ ИОКПБ №1 обязаны:

- участвовать в подготовке перечня персональных данных, обрабатываемых на ПЭВМ подразделения;
- готовить к утверждению списки работников, которых по своим должностным обязанностям необходимо допустить к работе с персональными данными в информационной системе ГУЗ ИОКПБ №1;
- контролировать целевое использование работниками ресурсов сети «Интернет»;
- контролировать выполнение пользователями общих правил работы на ПЭВМ и в локальной вычислительной сети ГУЗ ИОКПБ №1 (далее – ЛВС);
- выборочно контролировать характер исходящей информации, направляемой пользователями по электронной почте другим адресатам и принимать оперативные меры к соблюдению ими установленных требований по защите персональных данных;
- при обнаружении нарушений установленных требований по защите персональных данных, в результате которых вскрыты факты их разглашения, прекратить работы на рабочем месте, где обнаружены нарушения, доложить начальнику ГУЗ ИОКПБ №1 и поставить в известность начальника отдела ВЦ;
- назначать служебные расследования по фактам разглашения информации, содержащей персональные данные, или утери документов, содержащих такую информацию, по фактам нарушений пользователями правил, установленных для работы с персональными данными в ЛВС, а также нарушений требований по защите информации;
- обеспечивать условия для работы представителя отдела ВЦ при проверке в подразделении эффективности предусмотренных мер защиты информации;
- определять порядок передачи информации, содержащей персональные данные, другим подразделениям ГУЗ ИОКПБ №1, сторонним организациям и органам.

8.5. При приеме на работу работник предупреждается об ответственности за разглашение сведений, содержащих персональные данные, которые станут ему известными в связи с предстоящим выполнением своих служебных обязанностей.

8.6. Пользователь обязан:

- знать правила работы в ЛВС и принятые меры по защите ресурсов ЛВС (в части, его касающейся);
- при работе на своей рабочей станции (ПЭВМ) и в ЛВС выполнять только служебные задания;
- перед началом работы на ПЭВМ проверить свои рабочие папки на жестком магнитном диске, съемные магнитные носители информации на отсутствие вирусов с

помощью штатных средств антивирусной защиты, убедиться в исправности своей рабочей станции;

- при сообщениях программ о появлении вирусов немедленно прекратить работу, доложить начальнику отдела ВЦ и своему непосредственному начальнику;
- при обработке информации, содержащей персональные данные, использовать только зарегистрированные в журналах учета ГУЗ ИОКПБ №1 машинные носители информации (далее – МНИ);
- при необходимости использования неучтенных магнитных носителей, прежде всего, провести проверку этих носителей на отсутствие вирусов;
- выполнять предписания работника отдела ВЦ ответственного за защиту информации в ГУЗ ИОКПБ №1 (работников отдела ВЦ);
- представлять для контроля свою рабочую станцию (ПЭВМ) работникам отдела ВЦ;
- сохранять в тайне свой индивидуальный пароль, периодически, но не реже чем один раз в полгода, изменять его и не сообщать другим лицам;
- вводить пароль и другие учетные данные, убедившись, что клавиатура находится вне поля зрения других лиц;
- учет, размножение, обращение печатных материалов, содержащих персональные данные, проводить в соответствии с требованиями Инструкции по делопроизводству в ГУЗ ИОКПБ №1, утвержденной приказом главного врача ГУЗ ИОКПБ №1 от 22 ноября 2013 года № 209;
- при обнаружении различных неисправностей в работе компьютерной техники или ЛВС, недокументированных свойств в программном обеспечении, нарушений целостности пломб (наклеек, печатей), несоответствии номеров на аппаратных средствах сообщить в отдел ВЦ, администратору сети и поставить в известность руководителя подразделения.

Пользователю при работе запрещается:

- играть в компьютерные игры;
- приносить различные компьютерные программы и пытаться установить их на локальный диск компьютера без уведомления специалистов отдела ВЦ и администратора сети;
- перенастраивать программное обеспечение компьютера;
- самостоятельно вскрывать комплектующие рабочей станции (ПЭВМ);
- запускать на своей рабочей станции (ПЭВМ) или другой рабочей станции сети любые системные или прикладные программы, кроме установленных специалистами отдела ВЦ сети;
- изменять или копировать файл, принадлежащий другому пользователю, не получив предварительно разрешения владельца файла;
- оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации (при наличии), магнитные носители и распечатки, содержащие персональные данные;
- допускать к подключенной в сеть рабочей станции (ПЭВМ) посторонних лиц;
- производить копирование для временного хранения информации, содержащей персональные данные, на неучтенные носители;

- работать на рабочей станции (ПЭВМ) в сети с информацией, содержащей персональные данные, при обнаружении неисправностей станции (ПЭВМ), влияющих на защиту информации;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты информации, которые могут привести к утечке, блокированию, искажению или утере информации, содержащей персональные данные;
- отсылать по электронной почте информацию для решения личных проблем, а также информацию по просьбе третьих лиц без согласования с начальником отдела;
- запрашивать и получать из сети "Интернет" материалы развлекательного характера (игры, клипы и т.д.);
- запрашивать и получать из сети "Интернет" программные продукты, кроме случаев, связанных со служебной необходимостью. При этом необходимо согласование с начальником отдела и обеспечение процесса техническими специалистами отдела ВЦ.

8.7. Работники не могут использовать в личных целях персональные данные, ставшие известными им вследствие выполнения служебных обязанностей.

9. Порядок обработки персональных данных без использования средств автоматизации:

9.1.Обработка персональных данных без использования средств автоматизации (далее - неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.

9.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

9.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

9.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную

обработку персональных данных (при необходимости получения письменного согласия на обработку персональных данных);

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

9.5. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

9.6. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

9.7. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных - осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
- при необходимости уничтожения или блокирования части персональных данных - уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

9.8. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

9.9. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ.

9.10. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

III. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

10. Целью обработки персональных данных является:

1) осуществление возложенных на ГУЗ ИОКПБ №1 полномочий в сфере оказания специализированной стационарной психиатрической помощи.

2) организация деятельности ГУЗ ИОКПБ №1 для обеспечения соблюдения законов и иных нормативных правовых актов, реализации права на труд, права на пенсионное обеспечение и медицинское страхование работников.

IV. СОДЕРЖАНИЕ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

11. К персональным данным, обрабатываемым для достижения целей, указанных в подпункте 1 пункта 10 настоящих Правил относятся ПДн пациентов.

- Фамилия, имя, отчество;
- Дата и место рождения;
- Код территории проживании (район, город);
- Диагноз по МКБ-10;
- Номер медицинской карты;
- Место работы;
- Причины нетрудоспособности;
- Дата начала госпитализации и дата выписки.
- Цель направления;
- Инвалидность;
- Образование;
- Источник существования;
- Условия проживания;
- Исход лечения;
- Данные о состоянии здоровья;
- СНИЛС, полис медицинского страхования;
- Паспортные данные;
- Данные о пенсионных выплатах.

12. К персональным данным, обрабатываемым для достижения целей, указанных в подпункте 2 пункта 10 настоящих Правил относятся:

- Анкетные и биографические данные гражданина, включая адрес места жительства и проживания;
- Паспортные данные или данные иного документа, удостоверяющего личность и гражданство (включая серию, номер, дату выдачи, наименование органа, выдавшего документ);
- Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (включая серию, номер, дату выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, дату начала и завершения обучения);
- Сведения о трудовой деятельности, опыте работы, занимаемой должности, трудовом стаже, повышении квалификации и переподготовках;
- Сведения о номере, серии, дате выдачи трудовой книжки (вкладыша в неё) и записях в ней, содержание и реквизиты трудового договора (контракта);
- Сведения о составе семьи и наличии иждивенцев;
- Сведения о месте работы или учёбы членов семьи;
- Сведения о состоянии здоровья и наличии заболеваний (когда это необходимо в случаях, установленных законом);
- Сведения об отношении к воинской обязанности;

- Сведения о доходах и обязательствах имущественного характера, в том числе членов семьи;
- Сведения об идентификационном номере налогоплательщика;
- Сведения о социальных льготах и о социальном статусе;
- Сведения из страховых полисов обязательного (добровольного) медицинского страхования;
- Сведения о номере и серии страхового свидетельства государственного пенсионного страхования.

V. КАТЕГОРИИ СУБЪЕКТОВ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ

13. К субъектам, персональные данные которых обрабатываются, относятся:

1) граждане, находящиеся на стационарном лечении в ГУЗ ИОКПБ №1;
2) граждане, находящиеся в трудовых отношениях с ГУЗ ИОКПБ №1.

VI. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

14. Сроки обработки и хранения персональных данных определяются:

1) сроки хранения статкарты и истории болезни выбывшего из психиатрического стационара форма №066-1/у определены Приказом Минздрава СССР от 30 мая 1974 г. N 493 "О введении в действие "Перечня документов со сроками хранения Министерства здравоохранения СССР, органов, учреждений, организаций, предприятий системы здравоохранения" и приказом Минздрава СССР от 4 октября 1980 г. № 1030 и составляют 50 лет;

2) срок хранения документов по личному составу определен Приказом Министерства культуры Российской Федерации от 25.08.2010 г. №558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения» и составляет 75 лет;

3) иными требованиями законодательства Российской Федерации, нормативными правовыми актами ГУЗ ИОКПБ №1.

15. Особенности хранения персональных данных:

Если срок хранения персональных данных не установлен законодательством Российской Федерации, нормативными правовыми актами ГУЗ ИОКПБ №1 или договором, стороной которого или поручителем по которому является субъект персональных данных, то хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

VII. ПОРЯДОК УНИЧТОЖЕНИЯ ОБРАБОТАННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

16. Под уничтожением обработанных персональных данных понимаются действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных, или в результате которых уничтожаются материальные носители персональных данных.

17. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

18. Порядок уничтожения обработанных персональных данных.

- Уничтожению подлежат утратившие практическое значение и не имеющие исторической или иной ценности носители информации, содержащие персональные данные. При уничтожении таких носителей должно быть исключено ознакомление с ними посторонних лиц, неполное или случайное их уничтожение.
- Уничтожение производится путем сожжения, расплавления, дробления, растворения, химического разложения или превращения в мягкую бесформенную массу или порошок. Допускается уничтожение документов путем измельчения в бумажную сечку. Магнитные и фотографические носители уничтожаются сожжением, дроблением, расплавлением и другими способами, исключающими возможность их восстановления.
- Уничтожение обработанных персональных данных производится комиссионно, с составлением соответствующего акта. Состав комиссии назначается приказом главного врача ГУЗ ИОКПБ №1 сроком на 1 год. В комиссию назначаются лица, допущенные к работе с персональными данными и являющиеся экспертами в различных областях деятельности ГУЗ ИОКПБ №1, имеющие непосредственное отношение к уничтожаемым материалам.
- На документальные материалы, отобранные комиссией для уничтожения, составляется акт об уничтожении документов, который подписывается членами комиссии и утверждается главным врачом ГУЗ ИОКПБ №1.
- Отобранные и включенные в акт об уничтожении документальные материалы после их сверки членами комиссии хранятся отдельно от других материалов.
- Уничтожение документальных материалов до утверждения акта об уничтожении документов главным врачом ГУЗ ИОКПБ №1 запрещается.
- Уничтожение должно производиться в возможно короткий срок после утверждения главным врачом ГУЗ ИОКПБ №1 акта об уничтожении документов.

19. Без оформления акта уничтожаются: испорченные бумажные и технические носители, черновики и проекты документов и другие материалы, образовавшиеся при исполнении документов, содержащих персональные данные.

В процедуру уничтожения документов и носителей информации без составления акта входит проведение следующих мероприятий:

- разрывание листов, разрушение магнитного или иного технического носителя в присутствии исполнителя и руководителя подразделения, допущенных к обработке персональных данных;
- накапливание остатков носителей в опечатываемом ящике (урне);
- физическое уничтожение остатков носителей несколькими сотрудниками подразделения, допущенными к работе с персональными данными;
- внесение отметок об уничтожении в учетные формы документов и носителей.

Приложение 22
Утверждены приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ПРАВИЛА РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ В ГУЗ ИОКПБ №1

1. Настоящие Правила работы с обезличенными данными в ГУЗ ИОКПБ №1 (далее - Правила) устанавливают порядок проведения мероприятий в ГУЗ ИОКПБ №1 по обезличиванию персональных данных, порядок и условия работы с обезличенными данными.

2. Обезличивание персональных данных и работа с обезличенными данными в ГУЗ ИОКПБ №1 осуществляется в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон №152-ФЗ), постановлением Правительства РФ от 21 марта 2012 года № 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», настоящими Правилами и другими нормативными правовыми актами, касающимися обработки персональных данных.

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных Федеральным законом № 152-ФЗ.

4. Целью обезличивания персональных данных в ГУЗ ИОКПБ №1 является обеспечение защиты персональных данных граждан 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.

5. Обезличивание персональных данных может быть проведено для решения следующих задач:

- получения статистических данных;
- снижения ущерба от разглашения защищаемых персональных данных;
- снижения класса используемых информационных систем персональных данных.

Кроме того, обезличивание персональных данных может быть проведено по достижению сроков обработки или в случае утраты необходимости в достижении целей обработки, если иное не предусмотрено законодательством Российской Федерации.

5.1. В случае достижения целей обработки персональных данных или в случае утраты необходимости в их достижении, сотрудник ГУЗ ИОКПБ №1, обрабатывающий персональные данные, обязан:

- незамедлительно прекратить обработку персональных данных;
- обезличить соответствующие персональные данные в срок, не превышающий 30 дней с даты достижения целей обработки персональных данных или утраты необходимости достижения этих целей.

5.2. Персональные данные не обезличиваются в случаях, если:

- договором (соглашением), стороной которого или поручителем по которому является субъект персональных данных, предусмотрен иной порядок обработки персональных данных;
- законодательством установлены сроки обязательного архивного хранения материальных носителей персональных данных;
- в иных случаях, прямо предусмотренных законодательством.

5.3. В случае выявления недостоверности персональных данных, неправомерности действий с персональными данными сотрудник ГУЗ ИОКПБ №1, обрабатывающий персональные данные, обязан осуществить незамедлительное блокирование указанных персональных данных и в срок, не превышающий 3 рабочих дней с даты такого выявления, устранить допущенные нарушения.

В случае подтверждения факта недостоверности персональных данных сотрудник ГУЗ ИОКПБ №1, обрабатывающий персональные данные, уточняет персональные данные и снимает с них блокирование на основании документов, представленных:

- субъектом персональных данных (его законным представителем);
- уполномоченным органом по защите прав субъектов персональных данных;
- иными лицами.

5.4. В случае невозможности устранения допущенных нарушений сотрудник ГУЗ ИОКПБ №1, обрабатывающий персональные данные, в срок, не превышающий 10 рабочих дней с даты выявления неправомерности действий с персональными данными, обезличивает персональные данные.

Об устранении допущенных нарушений или об обезличивании персональных данных сотрудник ГУЗ ИОКПБ №1, обрабатывающий персональные данные, уведомляет субъекта персональных данных (его законного представителя) по форме уведомления об устранении допущенных нарушений или уведомления об уничтожении (Приложение 1, 2) и (или) уполномоченный орган по защите прав субъектов персональных данных по форме уведомления об устранении допущенных нарушений или уведомления об уничтожении (Приложение3, 4).

5.5. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных сотрудник ГУЗ ИОКПБ №1, обрабатывающий персональные данные, обязан прекратить обработку персональных данных и обезличить их в срок, не превышающий 30 рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено законодательством, договором или соглашением между ГУЗ ИОКПБ №1 и субъектом персональных данных. Об обезличивании персональных данных сотрудник ГУЗ ИОКПБ №1, обрабатывающий персональные данные, уведомляет субъекта персональных данных (его законного представителя).

6. Способы обезличивания:

6.1. К способам обезличивания персональных данных при условии дальнейшей обработки персональных данных относятся:

- уменьшение перечня обрабатываемых сведений, замена части сведений словными обозначениями, обобщение (понижение) точности некоторых сведений;
- деление сведений на части и обработка их в разных информационных системах, другие способы.

6.2. К способам обезличивания персональных данных в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей относятся:

- сокращение перечня персональных данных;
- уничтожение персональных данных.

6.3. Уничтожение части персональных данных, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных персональных данных, зафиксированных на материальном носителе (закрашиванием, вырезанием и т.д.).

7. Правила работы с обезличенными данными:
7.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.
7.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.
7.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо:

- использование паролей;
- использование антивирусных программ;
- соблюдение правил доступа в помещения, в которых ведётся обработка персональных данных;

7.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- хранения бумажных носителей в условиях, исключающих доступ к ним посторонних лиц;
- соблюдение правил доступа в помещения, в которых ведётся обработка персональных данных.

Приложение 1
к Правилам работы с обезличенными данными

Уведомление об устранении допущенных нарушений

Уважаемый(ая)_____
(фамилия, имя, отчество)

в связи с

_____

сообщаем Вам, что все допущенные нарушения при обработке Ваших персональных данных устранены.

« ____» _____ 20__ г _____ _____
(дата) (подпись) (расшифровка подписи)

Приложение 2
к Правилам работы с обезличенными данными

Уведомление об уничтожении

Уважаемый(ая)_____
(фамилия, имя, отчество)

в связи с

_____

сообщаем Вам, что Ваши персональные данные уничтожены.

« ____» _____ 20__ г _____ _____
(дата) (подпись) (расшифровка подписи)

Приложение 3
к Правилам работы с обезличенными данными

Уведомление об устранении допущенных нарушений

Настоящим уведомлением сообщаем Вам, что допущенные нарушения при обработке персональных данных, а именно

_____

(указать допущенные нарушения)

устранены.

« ____» _____ 20__ г _____ _____

(дата) (подпись) (расшифровка подписи)

Приложение 4
к Правилам работы с обезличенными данными

Уведомление об уничтожении

Настоящим уведомлением сообщаем Вам, что в связи с _____
персональные данные _____
(указать, чьи персональные данные)
уничтожены.

« ____» _____ 20__ г _____ _____
(дата) (подпись) (расшифровка подписи)

Приложение 23
Утвержден приказом главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ЖУРНАЛ
УЧЕТА ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Журнал начат «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал завершен «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал составлен на _____ листах

№ п/п	Сведения о запрашивающем лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных	Дата передачи/ отказа в предоставлении персональных данных	Подпись запрашиваю щего лица	Подпись ответственного сотрудника

Приложение 24
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 год № 121

1.Форма СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ ГУЗ ИОКПБ №1

_____
дата

_____, именуемый в дальнейшем «Субъект персональных данных»
Ф.И.О.

разрешает ГУЗ ИОКПБ № 1, в лице ответственного за обработку персональных данных далее «Оператор», обработку персональных данных, приведенных в пункте 2 настоящего согласия на следующих условиях:

1. В соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» субъект персональных данных дает согласие на обработку Оператором своих персональных данных, с целью:
   - исполнения трудового договора;
   - для обеспечения личной безопасности, защиты жизни и здоровья работника;
   - в целях ведения финансово-хозяйственной деятельности организации;
   - иное (необходимо точное указание целей)
   - _____

2. Перечень персональных данных, на обработку которых дается согласие (нужное подчеркнуть):
   - дата и место рождения;
   - биографические сведения;
   - сведения об образовании (образовательное учреждение, время обучения, присвоенная квалификация);
   - сведения о местах работы (город, название организации, должность, сроки работы);
   - сведения о семейном положении, детях (фамилия, имя, отчество, дата рождения):
   - сведения о месте регистрации, проживании;
   - контактная информация;
   - сведения о постановке на налоговый учет (ИНН);
   - сведения о регистрации в Пенсионном фонде (номер страхового свидетельства);
   - сведения об открытых банковских счетах;
   - иное (необходимо точное указание)
   - _____

3. Оператор вправе осуществлять следующие действия с указанными выше персональными данными путем автоматизированной обработки и обработки без использования средств автоматизации (нужное подчеркнуть):
   - сбор;
   - систематизацию; накопление;
   - хранение;
   - уточнение (обновление, изменение); использование; распространение/передачу;
   - блокирование;
   - уничтожение;
   - иное (необходимо точное указание)
   - _____

4. Субъект персональных данных имеет право на доступ к его персональным данным в порядке, определенном статьей 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

5. Срок действия данного согласия устанавливается на период: с 16.05.2016 бессрочно.

6. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

Данные об операторе персональных данных:
Наименование организации **ГУЗ ИОКПБ № 1**
Адрес оператора **664059, Иркутская обл, Иркутск г, Юбилейный мкр, дом № 11а**
Ответственный за обработку ПДн
Субъект персональных данных:
Фамилия, имя, отчество _____
Адрес _____
Паспортные данные _____

_____ _____
(подпись) (ФИО)

2. Форма СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ закреплена в приложении к Положению об обработке и защите персональных данных пациентов

Приложение 25
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ФОРМА ЗАЯВЛЕНИЯ СУБЪЕКТА ОБ ОТЗЫВЕ СОГЛАСИЯ

Главному врачу ГУЗ ИОКПБ №1

_____

И.О. Фамилия

_____

(адрес)

от_____

Ф.И.О. субъекта

_____

адрес, где зарегистрирован субъект

_____

номер основного документа, удостоверяющего его личность

_____

дата выдачи указанного документа

_____

наименование органа, выдавшего документ

ЗАЯВЛЕНИЕ

Прошу Вас _____

(прекратить обработку, блокировать/уточнить/изменить/уничтожить/устранить нарушения)

моих персональных данных в связи с _____

_____

_____

(указать причину)

«____»_____ 201__ г. _____ / _____ /

(подпись) (Фамилия И.О.)

Приложение 26
Утверждено приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

УВЕДОМЛЕНИЕ
ОБ ОБРАБОТКЕ (О НАМЕРЕНИИ ОСУЩЕСТВЛЯТЬ ОБРАБОТКУ)
ПЕРСОНАЛЬНЫХ ДАННЫХ

_____

(наименование структурного подразделения, фамилия и инициалы руководителя)

с целью _____

(цель обработки персональных данных)

осуществляет обработку: _____

(категории персональных данных)

принадлежащих:_____

(категории субъектов, персональные данные которых обрабатываются)

_____

Обработка вышеуказанных персональных данных осуществляется путем:

_____

(перечень действий с персональными данными, общее описание используемых способов обработки персональных данных)

_____

_____

Обработка осуществляется с использованием информационной системы обработки персональных данных (ИСПДн)

_____

(характеристики ИСПДн)

с применением мер обеспечения безопасности обработки персональных данных

_____

(описание принимаемых мер по обеспечению безопасности персональных данных при их обработке)

_____

_____

Дата начала обработки персональных данных: _____

Срок или условие прекращения обработки персональных данных:_____

_____

Ответственное лицо за обеспечение безопасности персональных данных в ГУЗ ИОКПБ №1 при их обработке как с использованием, так и без использования средств автоматизации: _____

(должность, фамилия, имя, отчество, контактный телефон)

Разработчик ИСПДн_____

(должность, фамилия, имя, отчество, контактный телефон)

_____ _____ /_____/

должность подпись, дата расшифровка подписи

Приложение 27
Утверждено приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

СОГЛАСИЕ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ СЧИТАТЬ СВЕДЕНИЯ ОБЩЕДОСТУПНЫМИ

Я,_____
(Ф.И.О.)

_____
(адрес субъекта)

_____
(номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе)

_____

даю согласие считать следующие персональные данные общедоступными:
_____
(перечислить персональные данные)
_____
_____

необходимых в целях информационного обеспечения при работе в _____,
расположенного по адресу:
_____
_____.

Согласен на совершение следующих действий с моими общедоступными персональными данными: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, уничтожение, удаление персональных данных следующими способами: автоматизированная обработка, обработка без использования средств автоматизации.

В случае отзыва согласия на обработку персональных данных, ГУЗ ИОКПБ №1 обязуется прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 дней.

Данное согласие действует с «__» _____ 201_ г. по «__» _____ 201_ г.

С правом отзыва настоящего согласия ознакомлен.

_____ «___» _____ 201__г.
(подпись)

Приложение 28
Утвержден приказом главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ЖУРНАЛ
РЕГИСТРАЦИИ КЛЮЧЕЙ ОТ СПЕЦ.ПОМЕЩЕНИЙ/ХРАНИЛИЩ
В ГУЗ ИОКПБ №1

Журнал начат «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал завершен «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал составлен на _____ листах

№ п/п	Регистрационный номер ключа	Номер экземпляра ключа (печати)	Номер (название) режимного помещения/ хранилища	Дата, ФИО, получившего ключ, подпись	Отметки ответственного пользователя криптосредств/ руководителя		Сведения об утрате/замене ключа (№ акта, служебной записки и т.п.)
					ФИО	Дата, подпись о получении дубликата ключа	

Приложение 29
Утвержден приказом главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ЖУРНАЛ
УЧЕТА МЕРОПРИЯТИЙ ПО КОНТРОЛЮ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ
В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГУЗ ИОКПБ №1

Журнал начат «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал завершен «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал составлен на _____ листах

Дата проведения мероприятия	Название мероприятия	Название ИС, в которой проводилось мероприятие	Ф.И.О. и должность лица, исполнившего мероприятие	Результат проведенного мероприятия

Приложение 30
Утвержден приказом главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ЖУРНАЛ
РЕЗЕРВИРОВАНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ
ГУЗ ИОКПБ №1

Журнал начат «____» _____ 201_ г.
Должность
_____/ _____/
подпись фамилия, имя, отчество
Журнал завершен «____» _____ 201_ г.
Должность
_____/ _____/
подпись фамилия, имя, отчество
Журнал составлен на _____ листах

№ п/п	Дата	Вид резервирования (полное, частичное)	Наименование резервируемого информационного ресурса	Количество (общий размер файлов)	Тип носителя	Серийный номер носителя информации	Ответственное лицо	Примечание

Приложение 31
Утвержден приказом главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

.

ЖУРНАЛ
УЧЁТА СЕРТИФИЦИРОВАННЫХ СРЕДСТВ
ЗАЩИТЫ ИНФОРМАЦИИ (СЗИ)

Журнал начат «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал завершен «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал составлен на _____ листах

№ п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Номер сертификата соответствия и дата его регистрации	Данные о продлении сертификата	Наименование организации, установившей СЗИ	Место установки	Дата установки	Дата вывода из эксплуатации	Подпись ответствен-ного лица

Приложение 32
Утвержден приказом главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ЖУРНАЛ
ОЗНАКОМЛЕНИЯ СОТРУДНИКОВ С ДОКУМЕНТАМИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ
В ГУЗ ИОКПБ №1

Журнал начат «____» _____ 201_ г.
Должность
_____/ _____/
подпись фамилия, имя, отчество
Журнал завершен «____» _____ 201_ г.
Должность
_____/ _____/
подпись фамилия, имя, отчество
Журнал составлен на _____ листах

Наименование док-та / Фамилия ознакамливающегося	Политика информационной безопасности	Концепция информационной безопасности	Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПДн	Перечень общедоступных персональных данных	Инструкция администратора информационной безопасности в ИС	Инструкция по работе ответственного за обеспечение безопасности персональных данных в ИСПДн	Инструкция сотрудника ответственного за организацию обработки ПДн в ИСПДн	Инструкция пользователя ИС	Инструкция по организации парольной защиты в ИС	Инструкция по организации антивирусной защиты в ИС	Инструкция по действиям персонала во внештатных ситуациях при обработке защищаемой информации в ИС	Инструкция по приему под охрану кабинетов	Правила рассмотрения запросов субъектов ПД или их представителей	Правила обработки ПДн	Порядок доступа сотрудников в помещения , в которых ведется обработка ПДн	Инструкция по работе с отчуждаемыми носителями защищаемой информации, в том числе с ключевыми носителями, в ИС	Инструкция о порядке работы при подключении к сетям общего пользования и (или) международного обмена	Положение об обработке и защите персональных данных пациентов	Положение о защите , порядке хранения и использования персональных данных работников

Приложение 33
Утвержден приказом главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ЖУРНАЛ
ИНСТРУКТАЖА СОТРУДНИКОВ С ДОКУМЕНТАМИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ (СЗИ) И СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ) В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГУЗ ИОКПБ №1

Журнал начат «____» _____ 201_ г.
Должность
_____/ _____/
подпись фамилия, имя, отчество
Журнал завершен «____» _____ 201_ г.
Должность
_____/ _____/
подпись фамилия, имя, отчество
Журнал составлен на _____ листах

Наименование док-та / Фамилия ознакамливающегося	О проведении работ с использованием СКЗИ	Руководящие документы ФСБ России в области зашиты ПДн с использованием СКЗИ	Инструкции по обращенино с СКЗИ	Эксплуатационная документация на СКЗИ VipNet Client	Эксплуатационная документация на СЗИ SecrretNet	Эксплуатационная документация на СЗИ SSEP	Эксплуатационная документация на испол. серт. ОС

Приложение 34
Утверждены приказом главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ПРАВИЛА ВЕДЕНИЯ ЖУРНАЛОВ В ЧАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

1. Настоящие Правила устанавливают порядок ведения и хранения специальных журналов в части защиты информации

2. При осуществлении видов деятельности, связанных с обеспечением безопасности защищаемой информации, любые операции, в результате которых изменяется уровень и класс защищенности информации, подлежат занесению в соответствующий журнал.

3. Руководитель ГУЗ ИОКПБ №1 назначает лиц, ответственных за ведение и хранение журналов.

4. Записи в журналах регистрации производятся лицом, ответственным за их ведение и хранение, шариковой ручкой (чернилами) с периодичностью, устанавливаемой руководителем ГУЗ ИОКПБ №1, но не реже одного раза в течение дня совершения операций с защищаемыми данными на основании документов, подтверждающих совершение этих операций.

5.Каждый журнал на первой странице обложки должен иметь следующую информацию:

- Название журнала
- Ответственный за ведение журнала
- Дата начала ведения журнала
- Дата окончания ведения журнала
- Место хранения в процессе работы
- Срок архивного хранения
- Место архивного хранения

6.Страницы журнала должны быть пронумерованы

7. Журналы должны быть сброшюрованы, пронумерованы и скреплены подписью главного врача ГУЗ ИОКПБ №1 и печатью ГУЗ ИОКПБ №1.

8. Записи должны вестись последовательно, не допускается делать записи справа или слева от уже сделанных записей.

9. Запрещается оставлять свободное место на страницах так, чтобы верхняя часть страницы была свободна, а внизу были сделаны записи.

10. Нумерация записей в журналах осуществляется в пределах календарного года в порядке возрастания номеров. Нумерация записей в новых журналах регистрации начинается с номера, следующего за последним номером в заполненных журналах.

11. Если в процессе ведения записей возникают записи на отдельных листах, эти листы, а так же документы или их копии, подтверждающие совершение операции с защищаемой информацией, должны быть подшиты или вклеены в журнал. Допускается подшить такие записи и документы в отдельную папку, которая хранится вместе с соответствующим журналом.

12. Запись в журналах каждой проведенной операции заверяется подписью лица, ответственного за их ведение и хранение, с указанием фамилии и инициалов.

13. Запрещается вносить записи карандашом и использовать замазку. Если запись сделана ошибочно, необходимо зачеркнуть ее так, чтобы была видна ошибочно сделанная запись, рядом внести правильную запись. Если ошибка была допущена при записи итоговых результатов, рядом с правильной записью необходимо поставить дату и подпись. Если записи были сделаны так, что места для внесения правильной записи нет, ошибочную запись необходимо зачеркнуть, выделить маркером, поставить рядом значок «*» и внести

правильную запись в конце текущей записи.

14. Исправления в журналах заверяются подписью лица, ответственного за их ведение и хранение. Подчистки и незаверенные исправления в журналах регистрации не допускаются.

15. Журнал регистрации хранится в металлическом шкафу (сейфе) в технически укрепленном помещении. Ключи от металлического шкафа (сейфа) и технически укрепленного помещения находятся у лица, ответственного за ведение и хранение журнала регистрации.

16. Заполненные журналы вместе с документами, подтверждающими осуществление операций, хранятся ГУЗ ИОКПБ №1 в течение 10 лет после внесения в них последней записи. По истечении указанного срока журналы подлежат уничтожению по акту, утверждаемому главным врачом ГУЗ ИОКПБ №1.

17. При реорганизации юридического лица журналы и документы, подтверждающие осуществление операций, передаются на хранение правопреемнику.

18. В случае ликвидации юридического лица журналы и документы, подтверждающие осуществление операций, передаются на хранение в государственный архив по месту нахождения юридического лица в соответствии с законодательством об архивном деле в Российской Федерации до истечения срока их временного хранения, установленного пунктом 16 настоящих Правил, после чего подлежат уничтожению в установленном порядке.

Приложение 35
Утвержден приказом главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ПОРЯДОК ДОСТУПА СОТРУДНИКОВ В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ГУЗ ИОКПБ №1

1. Настоящий Порядок доступа сотрудников ГУЗ ИОКПБ №1 в помещения, в которых ведется обработка персональных данных, разработан в соответствии с Федеральным законом от 27 июля 2006 г. № 152 ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением 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» и другими нормативными правовыми актами.

2. Персональные данные относятся к конфиденциальной информации. Сотрудники ГУЗ ИОКПБ №1, 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.

3. Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе, установлением правил доступа в помещения, где обрабатываются персональные данные в информационных системах персональных данных и без использования средств автоматизации.

4. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется в охраняемых помещениях.

5. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

6. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним

7. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только сотрудники ГУЗ ИОКПБ №1, уполномоченные на обработку персональных данных установленным образом.

8. Ответственными за организацию доступа в помещения ГУЗ ИОКПБ №1, в которых ведется обработка персональных данных, являются руководители структурных подразделений ГУЗ ИОКПБ №1.

9. Нахождение лиц в помещениях ГУЗ ИОКПБ №1, не являющихся уполномоченными лицами на обработку персональных данных, возможно только в присутствии уполномоченного сотрудника ГУЗ ИОКПБ №1 на время, ограниченное необходимостью решения вопросов, связанных с исполнением функций и (или) осуществлением полномочий структурного подразделения ГУЗ ИОКПБ №1.

10. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, проводится лицом, ответственным за обеспечения безопасности персональных данных.

Приложение 36
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ИНСТРУКЦИЯ ПО ОБРАЩЕНИЮ С СЕРТИФИЦИРОВАННЫМИ СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ГУЗ ИОКПБ №1

1. Общие положения

Настоящая Инструкция содержит описание порядка обращения с сертифицированными средствами криптографической защиты информации ФСБ России (далее – СКЗИ), рекомендации по размещению и хранению технических средств, на которые установлены СКЗИ, по проверке целостности установленного программного обеспечения (далее –ПО) СКЗИ, по использованию СКЗИ в различных информационных системах.

СКЗИ эксплуатируются в соответствии с правилами пользования ими, указанными в эксплуатационно-технической документации. Изменения условий эксплуатации СКЗИ, указанных в правилах пользования ими, допускаются исключительно по согласованию с ФСБ России.

Настоящая Инструкция разработана в соответствии с документами:

1.Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное Приказом ФСБ России №66 от 9 февраля 2005 года;

2.Приказ ФАПСИ при Президенте РФ №152 от 13 июня 2001 года «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

3.Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 центра ФСБ России 31 марта 2015 года №149/7/2-432.

2. Термины и сокращения

Лицензиат	Организация, обладающая лицензиями ФСБ России на
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
ПЭВМ	Персональная электронная вычислительная машина
СКЗИ	Средство криптографической защиты информации
ТС	Технические средства
ФСБ	Федеральная служба безопасности России
ЭТД	Эксплуатационная и техническая документация

3. Ответственные лица

В ГУЗ ИОКПБ №1, эксплуатирующей сертифицированные СКЗИ, назначены и закреплены распоряжением следующие лица:

Ответственный за обеспечение безопасности информации (далее - Администратор СКЗИ), на которого возлагаются задачи организации работ по:

- обеспечению корректного и безопасного функционирования СКЗИ;
- обеспечению корректной и безопасной эксплуатации СКЗИ;
- выработке соответствующих инструкций и ознакомление с ними пользователей СКЗИ;
- контролю работоспособности и соблюдения правил эксплуатации СКЗИ.

Пользователи СКЗИ, на которых возлагаются задачи по:

- соблюдению правил корректной и безопасной эксплуатации СКЗИ;
- обеспечению режима сохранности СКЗИ, ЭТД и ключевых документов, переданных им.

Администратор и Пользователи СКЗИ допускаются к работе с СКЗИ только после инструктажа и обучения правилам работы с СКЗИ.

Обучение Администратора СКЗИ правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты - Лицензиата. Документом, подтверждающим должную специальную подготовку Администратора СКЗИ и возможность его допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией соответствующего органа криптографической защиты на основании принятых от этих лиц зачетов по программе обучения.

Пользователей инструктирует и обучает Администратор СКЗИ.

Пользователи СКЗИ обязаны:

1. не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах;
2. соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
3. сообщать в орган криптографической защиты о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
4. 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. немедленно уведомлять орган криптографической защиты 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 сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

4. Размещение технических средств с СКЗИ

Организация режима в помещениях, где располагаются ТС с СКЗИ и ведется работа с носителями с персональной ключевой информацией, описана в правилах пользования СКЗИ.

В общем случае в отношении помещений ГУЗ ИОКПБ №1 должен быть установлен режим, определяющий:

- лицо, ответственное за помещение;
- перечень лиц, допущенных к работе в помещении и обслуживанию помещения;
- порядок доступа в помещение в рабочее и нерабочее время, в аварийных ситуациях (пожар, авария, стихийное бедствие и т.п.);
- порядок нахождения в помещении посторонних лиц (при необходимости их нахождения).

Окна помещений должны быть защищены от НСД посторонних лиц (в случае, если окна на 1 этаже, либо рядом с пожарными лестницами) металлическими решетками, а также от визуально просмотра ведущихся в помещениях работ (шторами или жалюзи).

Двери помещений должны быть оборудованы надежными замками, гарантирующими их надежное закрытие в нерабочее время.

Помещения должны быть оборудованы пожарной сигнализацией, для которых в ГУЗ ИОКПБ №1 установлен порядок периодической проверки их исправности.

Параметры сети электроснабжения помещений должны соответствовать требованиям инструкций по эксплуатации ТС и правилам техники безопасности.

Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать Администратору и Пользователям СКЗИ сохранность доверенных им СКЗИ, конфиденциальных документов и сведений, включая ключевую информацию, и свести к минимуму возможность неконтролируемого доступа к ним посторонних лиц.

Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища.

5. Хранение СКЗИ, ЭТД, ключевых документов, эталонных CD дисков

СКЗИ, ЭТД, ключевые документы, ключевые носители или аппаратные средства, к которым подключаются или в которые устанавливаются СКЗИ, эталонные CD-диски (диски, инсталлирующие программные СКЗИ), находящиеся у Администратора и Пользователей СКЗИ должны храниться в месте, исключающем возможность НСД к ним (сейф, шкаф индивидуального пользования с замком и т.п.), с пометкой в Журнале учета хранилищ. За их сохранность Администратор и Пользователей СКЗИ несут персональную ответственность.

6. Установка СКЗИ и программного обеспечения на ПЭВМ

Установка и настройка общесистемного, прикладного ПО и дополнительных средств защиты на ПЭВМ с СКЗИ производится Лицензиатом в соответствии с правилами установки и настройки СКЗИ и ПО, изложенными в ЭТД.

К установке и настройке СКЗИ и ПО предъявляются следующие общие требования:

- устанавливаемое ПО не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществить несанкционированный доступ к системным ресурсам;
- устанавливаемое ПО должно быть лицензионным;
- устанавливаемое ПО должно предусматривать организацию разрешительной системы доступа, при которой Администратор и Пользователи имеют свои атрибуты (учетную запись) для входа в систему и доступа к ресурсам;
- устанавливаемое ПО и СКЗИ, а также диски для их инсталляции должны подвергаться периодическому контролю целостности в соответствии с ЭТД;
- устанавливаемое ПО должно устанавливаться совместно с антивирусным ПО, базы которого должны своевременно и регулярно обновляться;
- устанавливаемое ПО не должно содержать возможностей, позволяющих модифицировать системные ресурсы (области памяти, программный код), передавать управление несанкционированным подпрограммам, повышать предоставленные привилегии, использовать недокументированные разработчиками возможности ОС).

7. Конфигурирование системного и прикладного программного обеспечения на ПЭВМ с СКЗИ

К ОС, в среде, которой планируется использовать СКЗИ, предъявляются следующие общие требования:

- на ПЭВМ должна быть установлена только одна лицензионная ОС, удовлетворяющая системным требованиям СКЗИ (запрещается использовать нестандартные, измененные или отладочные версии ОС);
- удаленное управление ОС должно быть запрещено или ограничено путем отключения всех служб, реализующих данные механизмы, или путем настроек, запрещающих фильтров для протоколов и портов удаленного управления ОС для всех узлов, кроме специально выделенных для этих целей;
- каждый пользователь должен иметь для входа в ОС свою учетную запись, длина пароля которой должна быть не менее 6 символов (см. п.8 Инструкции);
- учетная запись для гостевого входа (Guest) должна быть отключена;
- правом установки и настройки ОС и СКЗИ должен обладать только Администратор;
- все неиспользуемые ресурсы ОС должны быть отключены (протоколы, сервисы и т.п.);
- режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в ОС, права доступа к ресурсам должны быть назначены в объеме, необходимом для выполнения ими своих обязанностей;
- доступ должен быть максимально ограничен к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
  - системный реестр;
  - файлы и каталоги;
  - временные файлы;
  - журналы системы;
  - файлы подкачки;
  - кэшируемая информация (пароли и т.п.);
  - отладочная информация.
- регулярно должны устанавливаться пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), антивирусных баз;
- периодически должны исследоваться информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;
- должна быть исключена возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX), полученных из сети Internet, без проведения соответствующих проверок на предмет содержания в них программных закладок и сетевых вирусов (при подключении к сети Internet);
- на ПЭВМ с СКЗИ должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN сетей и т.п.) при подключению к сети Internet. При этом предпочтение должно отдаваться сертифицированным средствам защиты;
- должна быть реализована система аудита событий безопасности ОС, проводиться регулярный анализ результатов аудита;

Администратор СКЗИ должен осуществлять периодический контроль выполнения указанных требований, а также требований, приведенных в ЭТД.

Не допускается:

- обрабатывать на ПЭВМ, оснащенной СКЗИ, информацию, содержащую государственную тайну;
- осуществлять несанкционированное изменение аппаратной и программной конфигурации ПЭВМ (в том числе несанкционированное вскрытие), СКЗИ, ПО.

8. Защита СКЗИ от несанкционированного доступа

Защита СКЗИ от НСД включают в себя выполнение следующих мероприятий:

- на административном уровне (предпринимаемые руководством ГУЗ ИОКПБ №1 по обеспечению процессов ИБ (в частности по вопросам применения СКЗИ) ресурсами, управлением и контролем со стороны руководства);
- на организационном уровне (регламентация процессов охраны и режима допуска в отношении СКЗИ, ТС с СКЗИ, помещений, процессов обеспечения информационной безопасности (в частности при эксплуатации СКЗИ) и контроля эффективности, процессов обеспечения и поддержания компетентности персонала при работе с СКЗИ, распределение обязанностей и ответственности);
- на техническом уровне (обеспечение соблюдения правил эксплуатации и работоспособности СКЗИ).

Защита СКЗИ от НСД должна удовлетворять следующим общим требованиям:

- должна обеспечиваться на всех технологических этапах и во всех режимах функционирования СКЗИ, в том числе при проведении ремонтных и регламентных работ;
- должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль должен периодически выполняться Администратором СКЗИ на основе требований документации на средства защиты от НСД;
- должна исключать возможность несанкционированного не обнаруживаемого доступа к СКЗИ, ТС с СКЗИ, инсталлирующих и ключевых носителей изменения аппаратной части ТС с СКЗИ (путем опечатывания (опломбирования) системного блока и разъемов ПЭВМ, опечатывания замочных скважин мест сейфов, шкафов, ящиков для хранения).

Перечень сотрудников, допущенных к работе в помещениях, на ТС с СКЗИ и непосредственно СКЗИ, закреплен распоряжением ГУЗ ИОКПБ №1. Все они должны иметь соответствующий уровень компетентности и допускаться к работе только после инструктажа по обеспечению информационной безопасности с использованием СКЗИ и обучения эксплуатации СКЗИ.

Для регламентации входа в ОС, BIOS, при осуществления шифрования на пароле и т.д. Администратор СКЗИ основывается на Инструкции по организации парольной защиты в информационных системах ГУЗ ИОКПБ №1.

Администратор СКЗИ, а также Пользователи СКЗИ несут персональную ответственность за обеспечение режима конфиденциальности в отношении паролей доступа. Запрещается записывать пароли на материальные носители и хранить их в легкодоступных местах, в том числе на мониторе, рабочем столе или ящиках стола.

Периодичность смены пароля не должна превышать 1 год. Пароль должен быть изменен раньше плановой замены в случае его компрометации. Ответственность за своевременную смену пароля несет Администратор СКЗИ.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС. Средствами BIOS должна быть исключена возможность работы на ПЭВМ СКЗИ, если во время её начальной загрузки не проходят встроенные тесты.

9. Криптографическая защита

Порядок хранения и использования носителей ключевой информации с ключами электронной подписи должен исключать возможность несанкционированного доступа к ним.

Пользователи и Администратор СКЗИ, имеющие доступ к носителям ключевой информации, несут персональную ответственность за безопасность ключевой информации на них и обязаны обеспечивать её сохранность, неразглашение и нераспространение.

Во время работы с носителями ключевой информации доступ к ним посторонних лиц должен быть исключен.

При хранении ключевой информации СКЗИ в реестре Windows и на HDD ПЭВМ требования по хранению ключевых носителей распространяются на ПЭВМ.

В случае невозможности отчуждения ключевого носителя с ключевой информацией от ПЭВМ организационно-техническими мероприятиями должен быть исключен доступ нарушителей к ПЭВМ с ключами.

При хранении ключей на HDD ПЭВМ необходимо использовать парольную защиту.

Ключи должны обновляться с периодичностью, указанной в Правилах работы с СКЗИ.

Ключи на ключевых носителях (включая Touch Memory и смарт-карты), срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации.

Запрещается:

- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным
- вставлять ключевой носитель в считывающее устройство в режимах, не предусмотренных штатным режимом использования ключевого носителя;
- оставлять без контроля ТС, на которых эксплуатируется СКЗИ, после ввода ключевой информации;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.

Неиспользованные или выведенные из действия ключевые документы подлежат возвращению в орган криптографической защиты или по его указанию должны быть уничтожены на месте.

Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

10. Учет СКЗИ

Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету по установленным формам в соответствии с требованиями Положения ПКЗ-2005.

Администратор безопасности ведет учет поставки, установки и обслуживания в отношении следующих материалов:

- СКЗИ (СКЗИ);

- ЭТД (Э);
- ключевые документы - физические носители определенной структуры, содержащие ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию (КД);
- ключевые носители или аппаратные средства, к которым подключаются или в которые устанавливаются СКЗИ (А);
- эталонные CD диски (Д).

Учет ведется в Журнале поэкземплярного учета средств криптографической защиты информации (СКЗИ), эксплуатационной и технической документации к ним, ключевых документов.

Данный журнал должен храниться в месте, исключающем возможность несанкционированного доступа к нему (сейф, личный шкаф с замком и т.п.).

За ведение и хранение Журнала отвечает Администратор безопасности.

11. Контроль соблюдения условий эксплуатации и работоспособности СКЗИ

Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется:

1. обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ;
2. собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ;
3. ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

Приложение 37
Утвержден приказом главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ЖУРНАЛ
ПОЭКЗЕМПЛЯРНОГО УЧЕТА СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ), ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ)
В ГУЗ ИОКПБ №1

Журнал начат «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал завершен «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал составлен на _____ листах

N пп	Наименование	Серийные номера	Номера экземпляров	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников, производивших изъятие (уничтожение)	Дата изъятия (уничтожения)	
9	10	11	12	13	14	15

Приложение 38
Утвержден приказом главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ЛИЦЕВЫЕ СЧЕТА
ПОЛЬЗОВАТЕЛЕЙ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В
ГУЗ ИОКПБ №1

Журнал начат «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал завершен «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал составлен на _____ листах

№	ФИО пользователя СКЗИ	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Дата ввода в действие	Дата вывода из действия	Примечание
1	2	3	4	5	6	7	8
1							
2							
3							

Приложение 39
Утвержден приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

СПИСОК ПОМЕЩЕНИЙ,
ВЫДЕЛЕННЫХ ДЛЯ УСТАНОВКИ СКЗИ И ХРАНЕНИЯ КЛЮЧЕВЫХ ДОКУМЕНТОВ К НИМ

Для установки СКЗИ и хранения ключевых документов к ним выделены все кабинеты следующих отделов:

№ п/п	Название отдела	Адрес расположения
1.	Бухгалтерия (4 этаж административного корпуса)	г.Иркутск, м-н Юбилейный, 11А
2.	Расчетная группа (4 этаж административного корпуса)	г.Иркутск, м-н Юбилейный, 11А
3.	Отдел кадров (2 этаж административного корпуса)	г.Иркутск, м-н Юбилейный, 11А
4.	Плановый отдел (1 этаж административного корпуса)	г.Иркутск, м-н Юбилейный, 11А
5.	Отдел закупок (2 этаж административного корпуса)	г.Иркутск, м-н Юбилейный, 11А
6.	Касса (1 этаж административного корпуса)	г.Иркутск, м-н Юбилейный, 11А
7.	Кабинет диетврача (2 этаж административного корпуса)	г.Иркутск, м-н Юбилейный, 11А
8.	Пищеблок (кабинет кладовщика)	г.Иркутск, м-н Юбилейный, 11А
9.	Отдел АСУ (5 этаж административного корпуса)	г.Иркутск, м-н Юбилейный, 11А

Для хранения ключевых документов СКЗИ выделены следующие кабинеты:

№ п/п	Название отдела	Адрес расположения
1.	ВЦ (5 этаж административного корпуса)	г.Иркутск, м-н Юбилейный, 11А

Приложение 40
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ФОРМА - СПИСОК ЛИЦ ГУЗ ИОКПБ №1, ДОПУЩЕННЫХ К РАБОТЕ СО СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И ОТВЕТСТВЕННЫХ ЗА ЭКСПЛУАТАЦИЮ ПОЛУЧЕННОГО ЭКЗЕМПЛЯРА СКЗИ

К работе со средствами криптографической защиты допускаются следующие лица:

№ п/п	Ф.И.О.	Должность	ППО, в котором используются процедуры формирования и проверки ЭЦП	Имя рабочей станции, на котором установлен дистрибутив СКЗИ
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				

Приложение 41
Утвержден приказом главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

.

ЖУРНАЛ
ВЫДАЧИ НОСИТЕЛЕЙ С КЛЮЧЕВОЙ ИНФОРМАЦИЕЙ
В ГУЗ ИОКПБ №1

Журнал начат «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал завершен «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал составлен на _____ листах

№ п/п	Рег. №	Дата выдачи/сдачи	Выдано			Сдано		
			ФИО пользователя носителя с ключевой информацией	подпись пользователя носителя с ключевой информацией	подпись ответственного пользователя носителя криптосредств	ФИО пользователя носителя с ключевой информацией	подпись пользователя носителя с ключевой информацией	подпись ответственного пользователя криптосредств
1	2	3	4	5	6	7	8	9
1								

Приложение 42
Утвержден приказом главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ЖУРНАЛ
УЧЕТА, ХРАНЕНИЯ И ВЫДАЧИ МАШИННЫХ НОСИТЕЛЕЙ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ
В ГУЗ ИОКПБ №1

Журнал начат «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал завершен «____» _____ 201_ г.
Должность
_____/ _____ /
подпись фамилия, имя, отчество
Журнал составлен на _____ листах

№ п/п	Рег. №	Дата выдачи/сдачи	Тип носителя	Вид защищаемой информации	ФИО пользователя, получившего носитель	подпись пользователя, получившего носитель	подпись администратора информационной безопасности
1	2	3	4	5	7	8	9

Приложение 43
Утверждена приказом
главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ИНСТРУКЦИЯ ПО РАБОТЕ С ОТЧУЖДАЕМЫМИ НОСИТЕЛЯМИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ, В ТОМ ЧИСЛЕ С КЛЮЧЕВЫМИ НОСИТЕЛЯМИ, В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГУЗ ИОКПБ №1

1. Общие положения

1.1. Данная Инструкция содержит обязательные для всех сотрудников ГУЗ ИОКПБ №1 правила обращения с отчуждаемыми (съемными) носителями, использующимися для записи конфиденциальной информации и ключевыми носителями информации.

1.2. Под съемными носителями информации понимаются различные по физической структуре и конструктивному исполнению носители информации, используемые для записи и накопления информации с целью непосредственного ввода её в ЭВМ, обработки и передачи при помощи технических средств.

1.3. Под ключевым носителем информации понимается съемный носитель информации, на который записана уникальная секретная ключевая информация (идентификатор пользователя, закрытый ключ электронной подписи), используемая для подтверждения целостности, подлинности и авторства электронных документов, передаваемых в электронном виде.

1.4. Секретная ключевая информация, находящаяся на ключевом носителе, относится к категории сведений ограниченного распространения.

1.1. Данной инструкцией определяется порядок учета, хранения и обращения со съемными и ключевыми носителями (далее – носитель информации) информации и их утилизации. К съемным носителям информации относятся носители для однократной или многократной записи такие, как CD-R, CD-RW, DVD-R, DVD-RW, USB флеш-накопители и т.д.

1.2. Также данная инструкция регламентирует порядок обслуживания и обеспечение безопасности несъемных электронных носителей информации, к которым относятся базы данных на жестких магнитных дисках, содержащие информацию подлежащую защите.

1.3. Под безопасностью данных на электронных носителях информации понимается сохранение конфиденциальности, исключение несанкционированного проникновения либо иных действий, в том числе не имеющих злого умысла, которые могут привести к потере, искажению, изменению, копированию и другим нежелательным действиям с данными.

1.4. Организационное и техническое обеспечение безопасности конфиденциальной информации, хранящейся на электронных носителях информации во всех информационных системах (ИС) ГУЗ ИОКПБ №1, с использованием допустимых программно-аппаратных методов защиты, контроль за действиями сотрудников ГУЗ ИОКПБ №1 при работе с указанными носителями информации возлагается на администратора информационной безопасности.

1.5. Все находящиеся на хранении и в обращении носители информации конфиденциальной информации подлежат учёту. Каждый носитель информации с записанными на нем защищаемыми данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

1.6. Учет носителей информации осуществляет администратор информационной безопасности.

1.7. При обработке конфиденциальной информации пользователи ИС ГУЗ ИОКПБ №1 должны использовать только специально предназначенные для этого разделы (каталоги) электронных носителей информации или съемные маркированные носители информации.

1.8. При хранении носителей информации должны соблюдаться условия, обеспечивающие сохранность конфиденциальной информации и исключающие несанкционированный доступ к ней.

2. Обязанности работника

2.1. Работник обязан:

– при получении носителя информации, убедиться, что они правильно маркированы, и расписаться в соответствующем журнале.

– сдавать свой персональный ключевой носитель на временное хранение ответственному за обеспечение безопасности персональных данных на время длительного отсутствия на рабочем месте, в период отпуска и болезни и т.п.;

– сдавать свой съемный носитель на временное хранение администратору информационной безопасности на время длительного отсутствия на рабочем месте, в период отпуска и болезни и т.п.;

– в случае утери ключевого носителя немедленно сообщить об этом ответственному за обеспечение безопасности персональных данных и принять участие в служебном расследовании факта утери ключевого носителя;

– в случае утери съемного носителя немедленно сообщить об этом администратору информационной безопасности и принять участие в служебном расследовании факта утери съемного носителя;

– в случае перевода на другую работу, увольнения и т.п. он обязан сдать (сразу по окончании последнего сеанса работы) свой носитель информации администратору информационной безопасности и/или ответственному за обеспечение безопасности персональных данных под роспись в соответствующих журналах;

– хранить носитель конфиденциальной информации только в личном сейфе, либо в сейфе уполномоченного сотрудника.

2.2. Работникам запрещается:

– хранить носители конфиденциальной информации вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра в незапертом помещении или передавать на хранение другим лицам;

– выносить учтенные носители информации из служебных помещений для работы с ними на дому и т. д.

– передавать свой носитель информации другим лицам (кроме как для хранения уполномоченному лицу);

– оставлять носитель информации без личного присмотра;

– делать неучтенные копии с носителей информации.

2.3. При отправке или передаче конфиденциальных данных адресатам на съемные носители записываются только предназначенные адресатам данные.

2.4. Вынос съемных носителей, не содержащих персональных данных, для непосредственной передачи адресату осуществляется только с письменного разрешения

администратора информационной безопасности на основании запроса сторонней организации.

2.5. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения ответственного за обеспечение безопасности персональных данных в ИС ГУЗ ИОКПБ №1 на основании запроса сторонней организации с обязательной регистрацией в Журнале регистрации запросов на предоставление персональных данных.

2.6. Для защиты носителей информации от несанкционированного доступа, использования или повреждения во время транспортировки из одной организации в другую необходимо использовать надежных курьеров и транспорт, а также упаковку, защищающую носители от постороннего вмешательства и позволяющую выявить попытки ее вскрытия.

2.7. О фактах утраты носителей конфиденциальной информации либо разглашения содержащихся на них сведений немедленно ставится в известность руководителя ГУЗ ИОКПБ №1, администратора информационной безопасности и ответственного за обеспечение безопасности персональных данных. На утраченные носители составляется акт. Соответствующие отметки вносятся в журнал учета носителей информации.

2.8. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей конфиденциальной информации осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт по форме (Приложение1 к настоящей инструкции).

2.9. При изменении полномочий работника, его увольнения либо компрометации ключевого носителя, уничтожается все ключевая информация и подписывается акт об уничтожения ключевой информации с ключевых носителей (Приложение2).

2.10. Носители, на которые осуществляется резервное копирование защищаемой информации, должны регулярно (не реже одного раза в 6 месяцев) проверяться на отсутствие сбоев уполномоченными сотрудниками.

2.11. При повторном использовании носителей информации предыдущее содержимое должно надежно удаляться администратором информационной безопасности.

2.12. Повседневный и периодический контроль за действиями сотрудников ГУЗ ИОКПБ №1 при работе с носителями информации возлагается на администратора информационной безопасности.

3. Требования по работе с ключевым носителем

3.1. Для получения доступа к защищённым данным, хранящимся в памяти ключевого носителя, требуется ввести PIN-код (Personal Identification Number), являющегося аналогом пароля.

3.2. Пользователь должен выполнять следующие требования:

– изменить PIN-код сразу после получения ключевого носителя (USB-ключ/смарт-карту eToken). PIN-код необходимо хранить в тайне;

– соблюдать требования к ПИН-коду ключевого носителя, к его периодической смене.

3.3. При последовательном вводе более пяти неправильных PIN-кодов ключевой носитель блокируется. Для разблокировки ключевого носителя необходимо обратиться к администратору информационной безопасности.

3.4. В случае утраты ключевого носителя закрытый ключ восстановить невозможно. **Зашифрованная с помощью утерянного закрытого ключа информация восстановлению не подлежит.**

4. Ответственность

4.1. Сотрудник ГУЗ ИОКПБ №1 несет персональную ответственность за сохранность и правильное использование вверенного ему носителя информации.

4.2. За нарушение положений данной Инструкции к сотруднику может быть применена дисциплинарная ответственность, а так же ответственность, предусмотренная действующим законодательством РФ.

Приложение № 44
Утверждена
приказом главного врача ГУЗ ИОКПБ №1
от 29 марта 2017 года № 121

ИНСТРУКЦИЯ О ПОРЯДКЕ РАБОТЫ ПРИ ПОДКЛЮЧЕНИИ К СЕТЯМ ОБЩЕГО ПОЛЬЗОВАНИЯ И (ИЛИ) МЕЖДУНАРОДНОГО ОБМЕНА В ГУЗ ИОКПБ №1

1. Общие положения

1.1. Инструкция предназначена для сотрудников ГУЗ ИОКПБ №1 (пользователей), выполнение должностных обязанностей которых связано с использованием персональных компьютеров, и определяет их полномочия, обязанности и ответственность при использовании информационных ресурсов информационно-вычислительных сетей общего пользования (далее – ИВС ОП), в том числе сети Интернет, а также основные требования по обеспечению безопасности информации.

1.2. Руководители структурных подразделений ГУЗ ИОКПБ №1, пользователи и администраторы обязаны знать и выполнять нормативные правовые акты, затрагивающие вопросы информатизации, защиты информации и информационной безопасности в части соблюдения требований и ограничений по использованию информационных ресурсов.

1.3. Администратор информационной безопасности организуют ознакомление пользователей с настоящей Инструкции.

1.4. Доступ к ИВС ОП осуществляется с рабочей станции (РС) пользователя. Ответственность за действия на компьютере другого человека, несет пользователь РС с которого совершено это действие.

1.5. Основными угрозами безопасности информации при использовании ИВС ОП в ГУЗ ИОКПБ №1 являются:

– заражение информационно-вычислительных ресурсов ГУЗ ИОКПБ №1 программными вирусами;

– несанкционированный доступ внешних пользователей к информационно-вычислительным ресурсам ГУЗ ИОКПБ №1 (в т.ч. сетевые атаки);

– внедрение в автоматизированные информационные системы ГУЗ ИОКПБ №1 программных закладок;

– загрузка трафика нежелательной корреспонденцией (спамом);

– несанкционированная передача служебной информации ограниченного доступа сотрудниками ГУЗ ИОКПБ №1 в сеть Интернет (внутренний нарушитель);

– блокировка межсетевого взаимодействия с ИВС ОП путем нарушения целостности данных о настройках коммуникационного оборудования, обеспечивающего взаимодействие с ИВС ОП;

– нарушение целостности и достоверности открытых и общедоступных информационных ресурсов ГУЗ ИОКПБ №1, размещаемых в ИВС ОП.

1.6. Основными методами обеспечения безопасности информации при использовании ИВС ОП для предотвращения указанных угроз являются:

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов;

– использование сертифицированных средств защиты информации, в том числе антивирусных и криптографических;

– мониторинг вторжений (атак) из ИВС ОП, нарушающих или создающих предпосылки к нарушению установленных требований по защите информации, и анализ защищенности, предполагающий применение специализированных программных средств (сканеров безопасности);

– контроль информации, загружаемой или передаваемой в ИВС ОП;

– запрет обращения к нежелательным ресурсам ИВС ОП;

– шифрование информации при обмене с другими организациями при ее передаче по ИВС ОП, а также использование электронно-цифровой подписи для контроля целостности и подтверждения подлинности отправителя и/или получателя информации.

2. Доступ к Интернет-ресурсам

2.1. ГУЗ ИОКПБ №1 обеспечивает доступ пользователей сети к ресурсам ИВС ОП;

2.2. Открытие и контроль доступа регулируется администратором информационной безопасности. Подключение сотрудников ГУЗ ИОКПБ №1 к ИВС ОП осуществляется только на основании списка лиц, допущенных к ресурсам ИВС ОП.

2.3. Доступ к ресурсам ИВС ОП предоставляется сотрудникам ГУЗ ИОКПБ №1 только для выполнения ими прямых должностных обязанностей.

2.4. Самостоятельная организация дополнительных точек доступа к ИВС ОП (удаленный доступ, канал по локальной сети, GPRS и пр.) запрещена.

3. Основные ограничения при работе в сети Интернет

3.1. Пользователям запрещается:

– загружать, самостоятельно устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в его должностные обязанности;

– запрещается нецелевое использование подключения к ИВС ОП;

– осуществлять работу при отключенных средствах защиты информации, установленных на рабочей станции;

– допускать к работе посторонних лиц;

– передавать по сети ИВС ОП защищаемую информацию без использования средств шифрования;

– совершать любые попытки деструктивных действий по отношению к нормальной работе внутренней сети ГУЗ ИОКПБ №1 и ИВС ОП (рассылка вирусов, сетевые-атаки и т.п.);

– применять имена пользователей и пароли, используемые в ГУЗ ИОКПБ №1 в информационных системах за пределами ГУЗ ИОКПБ №1;

– использовать электронную служебную почту ГУЗ ИОКПБ №1 в личных целях;

– использовать для служебной переписки иную электронную почту отличную от служебной электронной почты ГУЗ ИОКПБ №1;

– посещать игровые, социальные, развлекательные и прочие сайты, не имеющие отношения к деятельности сотрудника ГУЗ ИОКПБ №1;

– посещать сайтов сомнительной репутации (сайты, содержащие нелегально распространяемое ПО и другие);

– посещение ресурсов трансляции потокового видео и аудио (веб-камеры, трансляция ТВ - и музыкальных программ в Интернете), создающих большую загрузку сети и мешающих нормальной работе остальных пользователей;

– игры на компьютере автономно и в сети;

– производить какие-либо действия с информацией, зараженной вирусом;

– подключаться к ресурсам ИВС ОП, используя рабочую станцию ГУЗ ИОКПБ №1 через не служебный канал доступа –сотовый телефон, модем, и др. устройства;

– создание личных веб-страниц и хостинг (размещение web- или ftp-сервера) на компьютере пользователя;

– нарушение закона об авторском праве: копирование и использование материалов и программ, защищенных законом об авторском праве;

– совершать действия, противоречащие законодательству, а также настоящей Инструкции.

3.2. Пользователь обязан:

– знать и уметь пользоваться антивирусным программным обеспечением. При обнаружении вируса он должен сообщить об этом администратору;

– информировать администратора о любых нарушениях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети;

– знать и соблюдать установленные правила работы в локальной сети (Приложение1 к настоящей Инструкции);

– знать и соблюдать установленные правила работы с электронной почтой (Приложение2 к настоящей Инструкции);

– знать и соблюдать установленные правила работы в сети Интернет (Приложение3 к настоящей Инструкции).

3.3. Пользователи несут персональную ответственность за содержание передаваемой, принимаемой и печатаемой информации.

3.4. Администратор информационной безопасности обязан:

– производить подключение к сети ИВС ОП только через специализированное устройство (Firewall) для обеспечения защиты информационной сети;

– знать и правильно использовать аппаратно - программные средства защиты информации и обеспечивать сохранность информационных ресурсов с помощью этих средств;

– оказывать методическую и консультационную помощь пользователям по вопросам, входящим в его компетенцию;

– ежемесячно вести учет и анализ использования ресурсов сети ИВС ОП по каждому пользователю;

– принимать меры для предотвращения и устранения нарушений требований настоящей инструкции пользователями и других негативных ситуациях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети.

3.5. Администратор имеет право:

– при обнаружение доступа к развлекательным сайтам, запретить доступ к сайту.

– при обнаружении использования пользователем программных продуктов, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети, запретить доступ к сети ИВС ОП;

– в целях обеспечения безопасности электронной системы ГУЗ ИОКПБ №1 производить выборочные и полные проверки всей электронной системы и отдельных файлов без предварительного уведомления работников.

4. Контроль использования ресурсов сети Интернет

4.1. В целях обеспечения информационной безопасности и безопасности внутренней сети ГУЗ ИОКПБ №1 администратор информационной безопасности осуществляет:

- контроль посещения ресурсов сети Интернет сотрудниками ГУЗ ИОКПБ №1, а также получаемых и передаваемых сотрудниками данных, в том числе и по электронной почте;
- контроль за соблюдением настоящей Инструкции;
- организацию и контроль за безопасным использованием ресурсов сети ИВС ОП.

5. Действия в нештатных ситуациях

5.1. При утрате (в том числе частично) подключения к сети ИВС ОП лицо, обнаружившее неисправность, сообщает об этом ответственному сотруднику за организацию подключения к сети Интернет;

5.2. При заражении компьютера вирусами его использование немедленно прекращается сотрудником, обнаружившим заражение. О сложившейся ситуации сообщается администратору информационной безопасности. Компьютер отключается от сети до момента очистки от всех вирусов.

Приложение1
к Инструкции о порядке работы
при подключении к сетям
общего пользования и (или)
международного обмена
в ГУЗ ИОКПБ №1

Правила по работе в локальной сети

1. Пользователи сети обязаны:
   - при доступе к внешним ресурсам сети, соблюдать правила, установленные администратором информационной безопасности(далее - администратор ИБ) для используемых ресурсов;
   - немедленно сообщать администратору ИБ об обнаруженных проблемах в использовании предоставленных ресурсов. Администратор ИБ, при необходимости, с помощью других специалистов, должны провести расследование указанных фактов и принять соответствующие меры;
   - не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы в сети;
   - обеспечивать беспрепятственный доступ администратора ИБ к сетевому оборудованию и компьютерам пользователей, для организации профилактических и ремонтных работ;
   - выполнять предписания администраторов ИБ, направленные на обеспечение безопасности сети;
   - в случае обнаружения неисправности (например, сильный посторонний шум или запах, необычное поведение затрудняющее работу) компьютерного оборудования или программного обеспечения, пользователь должен немедленно обратиться к администратору ИБ;
   - удалять с сетевых ресурсов устаревшие или не используемые файлы, владельцем или создателем которых он является;

2. Пользователи сети имеют право:
   - использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках. Администратор ИБ вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов;
   - обращаться к администратору ИБ по вопросам, связанным с распределением ресурсов компьютера. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов, или влияющие на загруженность или безопасность системы, должны санкционироваться администратором ИБ;
   - обращаться за помощью к администратору ИБ при решении задач использования ресурсов сети;
   - вносить предложения по улучшению работы с ресурсом.

3. Пользователям сети запрещено:
   - разрешать посторонним лицам пользоваться вверенным им компьютером;
   - использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей, без согласования с администратором ИБ;
   - самостоятельно устанавливать или удалять установленные администратором сетевые программы на компьютерах, подключенных к сети, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов;
   - повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю;
   - вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без согласования с администратором ИБ, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет;
   - самовольно подключать компьютер к сети, а также изменять IP-адрес компьютера, выданный администратором. Передача данных в сеть с использованием других IP адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах;
   - работать с каналоемкими ресурсами (видео, аудио, радио, чаты, файлообменные сети, torrent и др.) без согласования с администратором. При сильной перегрузке канала вследствие использования каналоемких ресурсов доступ пользователя вызвавшего перегрузку, может быть прекращен;
   - получать и передавать в сеть информацию, противоречащую действующему законодательству РФ и нормам морали общества, представляющую коммерческую или государственную тайну;
   - обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация;
   - использовать иные формы доступа к сети, за исключением разрешенных администратором ИБ;
   - осуществлять попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках и сетевом взломе;
   - использовать сеть для массового распространения рекламы (спам), коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.

Приложение2
к Инструкции о порядке работы
при подключении к сетям
общего пользования и (или)
международного обмена
в ГУЗ ИОКПБ №1

Правила работы с электронной почтой

1. Электронная почта предоставляется сотрудникам ГУЗ ИОКПБ №1 только для выполнения своих служебных обязанностей. Использование ее для пересылки файлов в личных целях запрещено. Создание или изменение параметров почтового ящика проводится администратором информационной безопасности на основании служебной записки;
2. На рабочем месте допускается использовать только ящики электронной почты, предоставленные ГУЗ ИОКПБ №1. Прямой доступ к другим почтовым системам может быть блокирован. Для получения писем с других систем допускается использовать переадресацию, которая может быть настроена с помощью администратора;
3. Все электронные письма, создаваемые и хранимые на компьютерах ГУЗ ИОКПБ №1, являются собственностью ГУЗ ИОКПБ №1 и не считаются персональными;
4. ГУЗ ИОКПБ №1 оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины;
5. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя;
6. Пользователи не должны позволять кому-либо посылать письма от чужого имени;
7. В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы;
8. Нельзя осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам);
9. Размер вложений у отправляемых писем не должен превышать 20Мб;
10. При работе с электронной почтой сотрудникам ГУЗ ИОКПБ №1 запрещается:

– использовать адрес электронной почты для оформления подписок;

– публиковать свой электронный адрес либо адреса других сотрудников ГУЗ ИОКПБ №1 на общедоступных Интернет-ресурсах (форумы, конференции и т.п.) за исключением случаев служебной необходимости;

– рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;

– распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

– распространять информацию, содержание и направленность которой запрещены международным и российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.;

– распространять информацию ограниченного доступа, предназначенную для служебного использования;

– предоставлять кому бы то ни было пароль доступа к своему почтовому ящику.

Приложение3
к Инструкции о порядке работы
при подключении к сетям
общего пользования и (или)
международного обмена
в ГУЗ ИОКПБ №1

Правила работы в сети Интернет

1. Пользователи используют программы для поиска информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей;
2. По использованию ресурсов Интернет необходимо ведение статистики;
3. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, протоколируются и могут использоваться для принятия решения о применении к нему санкций;
4. Сотрудникам ГУЗ ИОКПБ №1, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство РФ;
5. Все программы, используемые для доступа к сети Интернет, должны быть утверждены администратором информационной безопасности и на них должны быть настроены необходимые уровни безопасности;
6. Запрещено получать и передавать через сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения;
7. Запрещено обращаться к ресурсам сети Интернет несвязанных непосредственно с выполнением своих должностных обязанностей в рабочее время, а также к ресурсам с сомнительным содержанием;
8. Запрещается скачивать и запускать с любых ресурсов любые неизвестные исполняемые файлы без согласования с администратором информационной безопасности;
9. Запрещено использовать иные формы доступа к сети Интернет, за исключением разрешенных администратором ИБ;
10. Ответственность за все действия в сети Интернет, произведенные с рабочей станции, под именем и с паролем пользователя, им самим или другими физическими, или юридическими лицами и организациями, полностью лежит на самом пользователе.