Министерство социального развития, опеки и попечительства Иркутской области
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ КАЗЁННОЕ УЧРЕЖДЕНИЕ СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ
«ЦЕНТР ПОМОЩИ ДЕТЯМ, ОСТАВШИМСЯ БЕЗ ПОПЕЧЕНИЯ РОДИТЕЛЕЙ, г. Ангарска»

П Р И К А З

07 апреля 2022 г. № 69-од

г. Ангарск

О вводе в действие политики обработки персональных данных в информационных системах ОГКУСО ЦПД г. Ангарска

В целях обеспечения защиты информации в областном государственном казенном учреждении социального обслуживания «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска» (далее – Учреждение), в соответствии с Федеральными законами от 27.07.2006г. №149 «Об информатизации, информационных технологиях и о защите информации», от 27.07.2006г. №152 «О персональных данных», Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказом ФСТЭК России от 11 февраля 2013 года №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», руководствуясь Уставом

ПРИКАЗЫВАЮ:

1) Ввести в действие
- ПОЛИТИКУ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОГКУСО ЦПД Г. АНГАРСКА (приложение № 1);
- ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ (приложение № 2);
- ПРАВИЛА РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ (приложение № 3);
- ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ (приложение № 4);
- ПРАВИЛА РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ (приложение № 5);
- ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ (приложение № 6);
- ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ПОДЛЕЖАЩИХ ЗАЩИТЕ (приложение № 7);
- ПЕРЕЧЕНЬ ЗАЩИЩАЕМЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ (приложение № 8)

2) Заведующим отделений, главному бухгалтеру, заместителям директора, специалисту по кадрам Учреждения:

а) руководствоваться в работе настоящим приказом для определения правил и обязанностей по доступу к защищаемым объектам и соблюдению принятого режима безопасности персональных данных в информационных системах персональных данных Учреждения.

б) ознакомить сотрудников с настоящим приказом.

в) требовать соблюдение специалистами настоящего приказа при работе в государственных информационных системах Учреждения.

3)Контроль за исполнением настоящего приказа оставляю за собой.

Директор Олухова Н.А.

Приложение №1
к Приказу № 69-од от 07.04.2022 г.

ПОЛИТИКА
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОГКУСО ЦПД Г. АНГАРСКА

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Политика по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах ОБЛАСТНОГО ГОСУДАРСТВЕННОГО КАЗЕННОГО УЧРЕЖДЕНИЯ СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ "ЦЕНТР ПОМОЩИ ДЕТЯМ, ОСТАВШИМСЯ БЕЗ ПОПЕЧЕНИЯ РОДИТЕЛЕЙ, Г. АНГАРСКА" (далее – ОГКУСО ЦПД Г. АНГАРСКА) (далее – Политика) 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 (далее – ИС) ОГКУСО ЦПД Г. АНГАРСКА на протяжении всего жизненного цикла ИС.

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 ИС 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 ИС 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 ИС.

3.6. СЗПДн создается в три этапа:

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

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

Этап 3. Ввод ИС 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 ОГКУСО ЦПД Г. АНГАРСКА.

3.7.2. Создание комиссии по определению уровня защищенности ПДн при их обработке в ИС ОГКУСО ЦПД Г. АНГАРСКА.

3.7.3. Определение целей обработки ПДн ОГКУСО ЦПД Г. АНГАРСКА.

3.7.4. Определение перечня ИС ОГКУСО ЦПД Г. АНГАРСКА и состава ПДн, обрабатываемых в ИС.

3.7.5. Определение перечня обрабатываемых ОГКУСО ЦПД Г. АНГАРСКА 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 ИС (предлагаемых к использованию в ИС) общесистемных и прикладных программных средств.

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

3.7.9. Назначение ответственного за обеспечение безопасности ПДн в ИС (далее – Ответственный) для разработки и осуществления технических мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИС. Для каждой ИС 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 ИС (пользователей криптосредств).

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

3.7.12. Определение конфигурации и топологии ИС 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 ИС, включая условия их расположения.

3.7.14. Формирование технических паспортов ИС.

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 ИС, пользователя ИС, ответственного пользователя криптосредств);

– Раздел должностных инструкций сотрудников ОГКУСО ЦПД Г. АНГАРСКА 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 ОГКУСО ЦПД Г. АНГАРСКА.

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 ИС 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 ИС).

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 ИС (разработка моделей угроз безопасности ПДн при их обработке в ИС).

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 ИС.

Техническое задание на разработку СЗПДн должно содержать:

– обоснование разработки СЗПДн;

– исходные данные создаваемой (модернизируемой) ИС в техническом, программном,

информационном и организационном аспектах;

– уровень защищенности ПДн при их обработке в ИС;

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

– 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 ИС и/или не нейтрализуют всех угроз безопасности ПДн для данной ИС.

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 ОГКУСО ЦПД Г. АНГАРСКА. Применение технических мер должно быть регламентировано нормативным актом ОГКУСО ЦПД Г. АНГАРСКА.

3.8.3. Средства защиты информации, применяемые в ИС, 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 ИС ОГКУСО ЦПД Г. АНГАРСКА 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 ИС к обрабатываемой в ИС информации;

– подготовка эксплуатационной документации на используемые средства защиты информации;

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

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

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

– опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИС (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 ОГКУСО ЦПД Г. АНГАРСКА 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 ИС ОГКУСО ЦПД Г. АНГАРСКА 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.

4.4. В соответствии с п. 5.2 Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденных руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144, при необходимости использования при создании СЗПДн средств криптографической защиты информации к проведению работ по обеспечению безопасности ПДн ОГКУСО ЦПД Г. АНГАРСКА необходимо привлекать специализированные организации, имеющие лицензии ФСБ России на осуществление работ по распространению шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведения, составляющие государственную тайну, на осуществление технического обслуживания шифровальных (криптографических) средств, на осуществление работ по оказанию услуг в области шифрования информации, не содержащих сведений, составляющих государственную тайну.

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

5.1. Модернизация СЗПДн для функционирующих ИС ОГКУСО ЦПД Г. АНГАРСКА должна осуществляться в случае:

– изменения состава или структуры ИС или технических особенностей ее построения (изменения состава или структуры программного обеспечения, технических средств обработки ПДн, топологии ИС);

– изменения состава угроз безопасности ПДн в ИС;
– изменения уровня защищенности ПДн при их обработке в ИС;
– 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 ИС, состава угроз безопасности ПДн в ИС и уровня защищенности ПДн при их обработке в ИС, соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Результаты проверки оформляются актом проверки и утверждаются руководителем ОГКУСО ЦПД Г. АНГАРСКА.

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 Политике обработки персональных данных

План мероприятий по защите персональных данных
в ОГКУСО ЦПД Г. АНГАРСКА

№ 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 ИС)	В случае создания ИС, а также приведения имеющихся ИС 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
6.	Ведение журналов учета	Постоянно	

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
	отчуждаемых электронных носителей персональных данных, средств защиты информации		
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 ИС)
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, необходимых в целях выполнения требований законодательства в области персональных данных»
11.	Определение уровня защищенности ПДн при их обработке в ИС	При необходимости	Определение уровня защищенности ПДн при их обработке в ИС осуществляется при создании ИС, 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 ИС
13.	Аттестация (сертификация) СЗПДн или декларирование соответствия по требованиям безопасности ПДн	При необходимости	Проводится совместно с лицензиатами ФСТЭК
14.	Эксплуатация ИС и контроль безопасности ПДн	Постоянно	
15.	Понижение требований по защите ПДн путем сегментирования ИС, отключения от сетей общего пользования, обеспечения обмена между ИС с помощью сменных носителей, создания автономных ИС на выделенных АРМ и прочих	При необходимости	В случае создания ИС, а также приведения имеющихся ИС в соответствии с требованиями закона

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
	доступных мер		

ПРИЛОЖЕНИЕ № 2
к Политике обработке персональных данных

План внутренних проверок режима защиты персональных данных в ОГКУСО ЦПД Г. АНГАРСКА

№	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 ИС	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
к Приказу №_____от_____ года

ПРАВИЛА
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОГКУСО ЦПД Г. АНГАРСКА

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Правила обработки персональных данных в ОГКУСО ЦПД Г. АНГАРСКА (далее – Правила) устанавливают единый порядок обработки персональных данных в ОГКУСО ЦПД Г. АНГАРСКА.

2. Обработка персональных данных в ОГКУСО ЦПД Г. АНГАРСКА 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 Новосибирской 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 ОГКУСО ЦПД Г. АНГАРСКА.

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 ОГКУСО ЦПД Г. АНГАРСКА, а также полученные путем иных установленных законом способов, являются собственностью ОГКУСО ЦПД Г. АНГАРСКА и не могут быть использованы иначе, как в установленных законом случаях или с разрешения руководителя ОГКУСО ЦПД Г. АНГАРСКА.

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 ОГКУСО ЦПД Г. АНГАРСКА;
- 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 ОГКУСО ЦПД Г. АНГАРСКА в течение 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 ОГКУСО ЦПД Г. АНГАРСКА 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 ОГКУСО ЦПД Г. АНГАРСКА 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 ОГКУСО ЦПД Г. АНГАРСКА или его заместителя, отвечающего за защиту информации в ОГКУСО ЦПД Г. АНГАРСКА.

8.3. Заместители директора ОГКУСО ЦПД Г. АНГАРСКА, работники ОГКУСО ЦПД Г. АНГАРСКА осуществляющие обработку персональных данных (далее - пользователи) обязаны контролировать и выполнять предусмотренные в ОГКУСО ЦПД Г. АНГАРСКА меры по защите информации, содержащей персональные данные.

8.4. Заместители директора ОГКУСО ЦПД Г. АНГАРСКА 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 ОГКУСО ЦПД Г. АНГАРСКА;
- контролировать целевое использование работниками ресурсов сети «Интернет»;
- контролировать выполнение пользователями общих правил работы на ПЭВМ и в локальной вычислительной сети ОГКУСО ЦПД Г. АНГАРСКА (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 ОГКУСО ЦПД Г. АНГАРСКА и поставить в известность начальника отдела информатизации и защиты информации ОГКУСО ЦПД Г. АНГАРСКА;
- 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 заместителя директора по информатизации ОГКУСО ЦПД Г. АНГАРСКА при проверке в подразделении эффективности предусмотренных мер защиты информации;

- определять порядок передачи информации, содержащей персональные данные, другим подразделениям ОГКУСО ЦПД Г. АНГАРСКА, 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 информатизации и защиты информации ОГКУСО ЦПД Г. АНГАРСКА и своему непосредственному начальнику;
- при обработке информации, содержащей персональные данные, использовать только зарегистрированные в журналах учета ОГКУСО ЦПД Г. АНГАРСКА машинные носители информации (далее – МНИ);
- при необходимости использования неучтенных магнитных носителей, прежде всего, провести проверку этих носителей на отсутствие вирусов;
- выполнять предписания работника отдела информатизации и защиты информации ОГКУСО ЦПД Г. АНГАРСКА ответственного за защиту информации в ОГКУСО ЦПД Г. АНГАРСКА (работников отдела информатизации и защиты информации ОГКУСО ЦПД Г. АНГАРСКА);
- представлять для контроля свою рабочую станцию (ПЭВМ) работникам отдела информатизации и защиты информации ОГКУСО ЦПД Г. АНГАРСКА;
- 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 ОГКУСО ЦПД Г. АНГАРСКА;
- 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 информатизации и защиты информации ОГКУСО ЦПД Г. АНГАРСКА, 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 информатизации и защиты информации ОГКУСО ЦПД Г. АНГАРСКА 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 информатизации и защиты информации ОГКУСО ЦПД Г. АНГАРСКА 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 информатизации и защиты информации ОГКУСО ЦПД Г. АНГАРСКА.

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 ОГКУСО ЦПД Г. АНГАРСКА полномочий в сфере передачи персональных данных в федеральную информационную систему «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении».

IV. СОДЕРЖАНИЕ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

1) фамилия, имя и отчество;

2) СНИЛС;

3) место рождения;

4) пол получателя;

5) сведения об образовании (включая серию, номер, дачу выдачи аттестата об окончании образовательного учреждения)

V. КАТЕГОРИИ СУБЪЕКТОВ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ

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

1) граждане, получившие документы об образовании в общеобразовательных организациях.

VI. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

13. Сроки обработки и хранения персональных данных определяются:

1) сроки хранения и обработки персональных данных согласно федеральному закону «О персональных данных» №152 от 27.07.2006г. должны быть не дольше, чем этого требуют цели обработки персональных данных;

2) иными требованиями законодательства Российской Федерации, нормативными правовыми актами ОГКУСО ЦПД Г. АНГАРСКА.

14. Особенности хранения персональных данных:

Если срок хранения персональных данных не установлен законодательством Российской Федерации, нормативными правовыми актами ОГКУСО ЦПД Г. АНГАРСКА 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

15. 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.

16. 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.

17. 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 директора ОГКУСО ЦПД Г. АНГАРСКА сроком на 1 год. В комиссию назначаются лица, допущенные к работе с персональными данными и являющиеся экспертами в различных областях деятельности ОГКУСО ЦПД Г. АНГАРСКА, имеющие непосредственное отношение к уничтожаемым материалам.

- На документальные материалы, отобранные комиссией для уничтожения, составляется акт об уничтожении документов, который подписывается членами комиссии и утверждается директором ОГКУСО ЦПД Г. АНГАРСКА.
- 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 директором ОГКУСО ЦПД Г. АНГАРСКА запрещается.
- Уничтожение должно производиться в возможно короткий срок после утверждения директором ОГКУСО ЦПД Г. АНГАРСКА акта об уничтожении документов.

18. 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 №3
к Приказу № 69-од от 07.04.2022 г.

ПРАВИЛА РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ ОГКУСО ЦПД Г. АНГАРСКА

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей ОГКУСО ЦПД Г. АНГАРСКА (далее - Правила) устанавливают единый порядок рассмотрения запросов субъектов персональных данных или их представителей в ОГКУСО ЦПД Г. АНГАРСКА.

2. Рассмотрение запросов субъектов персональных данных или их представителей в ОГКУСО ЦПД Г. АНГАРСКА 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 ОГКУСО ЦПД Г. АНГАРСКА.

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

- граждане, обратившиеся в ОГКУСО ЦПД Г. АНГАРСКА с жалобами, заявлениями и по другим вопросам, касающимся установленной сферы деятельности;
- граждане, претендующие на замещение должности государственной гражданской службы и должности технического (рабочего) персонала в ОГКУСО ЦПД Г. АНГАРСКА;
- граждане, замещающие (замещавшие) должности государственной гражданской службы и должности технического (рабочего) персонала в ОГКУСО ЦПД Г. АНГАРСКА.

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 недолжны 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 №4
к Приказу № 69-од от 07.04.2022 г.

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 ОГКУСО ЦПД Г. АНГАРСКА

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 ОГКУСО ЦПД Г. АНГАРСКА (далее – Правила) устанавливают порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ОГКУСО ЦПД Г. АНГАРСКА.

2. Осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ОГКУСО ЦПД Г. АНГАРСКА 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 ОГКУСО ЦПД Г. АНГАРСКА (далее – ответственный за организацию обработки) в ходе мероприятий по обработке персональных данных.

Ответственный за организацию обработки имеет право:

- запрашивать у сотрудников ОГКУСО ЦПД Г. АНГАРСКА 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 руководителю ОГКУСО ЦПД Г. АНГАРСКА предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить руководителю ОГКУСО ЦПД Г. АНГАРСКА 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 ОГКУСО ЦПД Г. АНГАРСКА, в состав которой входят работники ОГКУСО ЦПД Г. АНГАРСКА, допущенные к обработке персональных данных.

Плановый внутренний контроль соответствия обработки персональных данных установленным требованиям в ОГКУСО ЦПД Г. АНГАРСКА проводится на основании утвержденного руководителем ОГКУСО ЦПД Г. АНГАРСКА 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 ОГКУСО ЦПД Г. АНГАРСКА 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 ОГКУСО ЦПД Г. АНГАРСКА докладывает ответственный за организацию обработки либо председатель комиссии.

Приложение № 5
к Приказу № 69-од от 07.04.2022 г.

ПРАВИЛА
РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ В ОГКУСО ЦПД Г. АНГАРСКА

1. Настоящие Правила работы с обезличенными данными в ОГКУСО ЦПД Г. АНГАРСКА (далее - Правила) устанавливают порядок проведения мероприятий в ОГКУСО ЦПД Г. АНГАРСКА по обезличиванию персональных данных, порядок и условия работы с обезличенными данными.

2. Обезличивание персональных данных и работа с обезличенными данными в ОГКУСО ЦПД Г. АНГАРСКА 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 ОГКУСО ЦПД Г. АНГАРСКА 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 ОГКУСО ЦПД Г. АНГАРСКА, 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 ОГКУСО ЦПД Г. АНГАРСКА, 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 ОГКУСО ЦПД Г. АНГАРСКА, 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 ОГКУСО ЦПД Г. АНГАРСКА, 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 ОГКУСО ЦПД Г. АНГАРСКА, 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 (Приложение №3, 4).

5.5. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных сотрудник ОГКУСО ЦПД Г. АНГАРСКА, 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 ОГКУСО ЦПД Г. АНГАРСКА и субъектом персональных данных. Об обезличивании персональных данных сотрудник ОГКУСО ЦПД Г. АНГАРСКА, 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

_____
указать уполномоченный орган

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

_____
указать уполномоченный орган

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 № 6
к Приказу № 69-од от 07.04.2022 г.

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ
ОГКУСО ЦПД Г. АНГАРСКА

1. АИС Финансово-хозяйственная деятельность (АИС ФХД)

2. АИС «Электронный социальный реестр населения»

Приложение №7
к Приказу № 69-од от 07.04.2022 г.

ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ПОДЛЕЖАЩИХ ЗАЩИТЕ В ОГКУСО ЦПД Г. АНГАРСКА

Конфиденциальность персональных данных - обязательное для соблюдения сотрудниками ОГКУСО ЦПД Г. АНГАРСКА требование: не допускать распространения персональных данных без согласия субъекта персональных данных или наличия иного законного основания.

Защищаемыми информационными ресурсами в информационной системе персональных данных (далее ПДн) ОГКУСО ЦПД Г. АНГАРСКА являются:

1. ПДн обрабатываемые в автоматизированном виде:
- фамилия, имя и отчество;
- СНИЛС;
- Паспортные данные;
- Информация о детях;
- дата рождения;
- пол получателя;
- сведения об образовании
- ИНН

Приложение № 8
к Приказу № 69-од от 07.04.2022 г.

ПЕРЕЧЕНЬ ЗАЩИЩАЕМЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОГКУСО ЦПД Г. АНГАРСКА

Защищаемыми информационными ресурсами в информационных системах ОГКУСО ЦПД Г. АНГАРСКА являются:

1. Данные, содержащиеся в информационных системах ОГКУСО ЦПД Г. АНГАРСКА, в том числе информация:
   – ПДн не сотрудников;
2. Технологическая информация, подлежащая защите, включает:
   – управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
   – сведения о проведенных служебных проверках, дисциплинарных взысканиях;
   – информация о квалификационных экзаменах;
   – сведения о кадровом резерве;
   – технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
   – информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
   – информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;
   – информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
   – служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.
3. Программно-технические средства включают в себя:
   – общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);
   – резервные копии общесистемного программного обеспечения;
   – инструментальные средства и утилиты систем управления ресурсами ИС;
   – аппаратные средства обработки ПДн (АРМ и сервера);
   – сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).
4. Средства защиты данных состоят из аппаратно-программных средств, включают в себя:
   – средства управления и разграничения доступа пользователей;

- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты;
- средства анализа защищенности;
- средства обнаружения вторжений
- средства межсетевого экранирования;
- средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена.

5. Каналы информационного обмена и телекоммуникации, по которым передаются обрабатываемая и технологическая информация.

6. Объекты и помещения, в которых происходит обработка технологической информации, установлены технические средства обработки и защиты.

7. В информационные системы ОГКУСО ЦПД Г. АНГАРСКА могут включаться иные сведения, за исключением сведений, отнесенных к государственной тайне.

УТВЕРЖДАЮ
Директор ОГКУСО «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска»
_____ Н.А. Олухова
«15» 10 2024 г.

Инструкция по организации парольной защиты в локальных вычислительных сетях
Областного государственного казенного учреждения социального обслуживания «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска»

1. Общие положения

1.1. Инструкция по организации парольной защиты (далее Инструкция) регламентирует установку, смену и прекращение действия паролей, блокировку учетных записей пользователей в локальной вычислительной сети (далее - ЛВС) Областного государственного казенного учреждения социального обслуживания «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска» (далее — учреждение).

1.2. Пароль пользователя ЛВС — это комбинация символов (буквы, цифры, специальные символы), известная только пользователю ЛВС, предназначенная для аутентификации пользователя в операционной системе автоматизированного рабочего места и в ЛВС.

1.3. Должностные лица, оформляемые на работу, должны быть ознакомлены специалистом по кадрам с настоящей инструкцией под подпись в журнале ознакомления.

1.4. Журналы ознакомления с настоящей инструкцией хранятся у специалиста по кадрам учреждения.

2. Требования к паролям, используемым в ЛВС

2.1. Пользователям ЛВС запрещается использовать пароли, имеющие в своем составе:

– имя, отчество или фамилию пользователя, или близких родственников;

идентификатор входа (имя пользователя в операционной системе);

– какую-либо информацию о пользователе (номера телефонов, номера в личных документах, номер или марка автомобиля, почтовый адрес и Т.Д.);

повторяющиеся наборы цифр, букв, символов.

2.2. Пользователи ЛВС обязаны при формировании паролей включать вих состав:

- строчные и прописные буквы;цифры;

- специальные символы.

2.3. Пароль должен содержать не менее 8 символов.

2.4. Новый пароль пользователя ЛВС должен отличаться от четырехпредыдущих паролей.

3. Порядок смены личных паролей, используемых в ЛВС

3.1. Первоначальную установку временного пароля производит администратор ЛВС, пользователь производит смену пароля при первом входе в операционную систему.

3.2. Пользователь обязан не реже одного раза в квартал самостоятельно осуществлять смену пароля.

3.3. При формировании пароля пользователь обязан руководствоваться разделом 2 настоящей Инструкции.

3.4. В случае компрометации пароля (либо подозрения на компрометацию) необходимо немедленно сообщить об этом ведущему системному администратору и изменить пароль.

3.5. В случае прекращения полномочий пользователя ЛВС (увольнение, перевод на другую должность и т. п.) в течение одного рабочего дня руководитель соответствующего структурного подразделения информирует ведущему системного администратора для организации блокирования учетной записи пользователя.

4. Обязанности пользователя КНВС и ЛВС

4.1. Пользователь ЛВС обязан:

- сохранять свой пароль в тайне;

- своевременно производить смену пароля;

- информировать администратора КИВС и ЛВС обо всех случаях

компрометации пароля;

- информировать администратора КИВС и ЛВС обо всех случаях нарушения Инструкции.

4.2. Пользователю КИВС и ЛВС запрещается:

- передавать свой пароль другим лицам;
- записывать свой пароль на бумажных или электронных носителях;
- пересылать свой пароль в электронных и иных открытых сообщениях.

5. Ответственность пользователя ЛВС

5.1. Нарушение требований Инструкции является дисциплинарным проступком.

5.2. За нарушение требований Инструкции, пользователь ЛВС может быть привлечен к дисциплинарной ответственности.

5.3. В случаях, предусмотренных законодательством Российской Федерации, за нарушение требований Инструкции пользователь ЛВС может быть привлечен к административной или уголовной ответственности.

6. Контроль за соблюдением пользователями ЛВС Инструкции по организации парольной защиты в ЛВС

6.1. Контроль за соблюдением требований Инструкции к паролям осуществляет администратор безопасности ЛВС путем установления групповых политик в ЛВС, а также в ходе проверки выполнения Инструкции пользователями ЛВС.

6.2. Контроль за соблюдением пользователями ЛВС иных требований Инструкции осуществляется их непосредственными руководителями в пределах их компетенции.

УТВЕРЖДАЮ
Директор ОГКУСО «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска»
_____ Н.А. Олухова
«13» 10 2024 г.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Областного государственного казенного учреждения социального обслуживания «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска»

1. Общие положения

1.1. Пользователь ИСПДн (далее Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является сотрудник Областного государственного казенного учреждения социального обслуживания «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска» (далее - учреждение), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, локальными актами учреждения, руководящими и нормативными документами в сфере защиты конфиденциальной информации и персональных данных, в частности.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2. Обязанности пользователя

Пользователь обязан:

2.1. 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.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в соответствии с правилами разграничения доступа.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена — Интернет и других.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью учреждения, а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному администратору безопасности.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн.

2.9. Пользователям запрещается:

- Разглашать защищаемую информацию третьим лицам.
- Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.
- Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
- Несанкционированно открывать общий доступ к папкам на своей рабочей станции.
- Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.
- Отключать (блокировать) средства защиты информации.

- Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.

- Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

- Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш windows + L или Ctrl+A1t+Delete раздел Блокировка (Заблокировать).

2.11. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках, возложенных на него функций.

2.12. Не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты;

2.13. Соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним;

2.14. Сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

2.15. Немедленно уведомлять оператора о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

2.16. Сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящими Требованиями, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;

2.17. Не разглашать информацию о ключевых документах;

2.18. Не допускать снятие копий с ключевых документов;

2.19. Не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;

2.20. Не допускать записи на ключевой носитель посторонней информации;

2.21. Не допускать установки ключевых документов в другие ПЭВМ.

УТВЕРЖДАЮ
Директор ОГКУСО «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска»
_____ Н.А. Олухова
«15» 10 2024 г.

Инструкция пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций

в областном государственном казенном учреждении социального обслуживания «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска»

СОДЕРЖАНИЕ:

1. Основные термины, сокращения и определения

Администратор ИСПДн— технический специалист, ведущий системный администратор учреждения, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения и оборудования вычислительной техники.

Администратор безопасности ИСПДн - технический специалист, ведущий системный администратор учреждения и обеспечивает правильность использования и нормальное функционирование установленных систем защиты информации.

Оператор ИСПДн - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

ИСПДн — информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Носитель информации — любой материальный объект, используемый для хранения и передачи электронной информации.

ПК — персональный компьютер.

ПО — программное обеспечение вычислительной техники.

Пользователь — работник учреждения, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

2. Назначение и область действия

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн областного государственного казенного учреждения социального обслуживания «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска» (далее — учреждение), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз. Задачей данной Инструкции является:

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

Действие настоящей Инструкции распространяется на всех пользователей учреждения, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

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

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

3. Порядок реагирования на аварийную ситуацию

3.1. Действия при возникновении аварийной ситуации

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении 1.

Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные реагирование сотрудники учреждения (Администратор безопасности, Администратор Оператор ИСПДн) 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.

3.2. 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 ИСПДн 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 ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

отказ элементов ИСПДн 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.

отсутствие Администратора ИСПДн и Администратора безопасности более чем на сутки из-за:

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

Уровень 3 — Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПДн 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.

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

4.1. Технические меры.

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

- системы жизнеобеспечения;

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

Системы жизнеобеспечения ИСПДн включают:

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

Все критичные помещения учреждения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в Положении о порядке учета, хранения и обращения со съемными носителями персональных данных.

4.2. Организационные меры.

Ответственные за реагирование сотрудники ознакомляют всех сотрудников Учреждения, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу.

По окончанию ознакомления сотрудник расписывается в журнале, предоставляемом Ответственным за реагирование сотрудником. Подпись сотрудника должна соответствовать его подписи в документе, удостоверяющем его личность.

Должно быть проведено обучение должностных лиц Учреждения, имеющих доступ к ресурсам ИСПДн, 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.

Администраторы ИСПДн и Администраторы безопасности должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

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.

Приложение № 1

Таблица 1 – источники угроз

	Технологические угрозы
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
4	Химический выброс в атмосферу
	Внешние угрозы
5	Массовые беспорядки
6	Сбои общественного транспорта
7	Эпидемия
8	Массовое давление персонала
	Стихийные бедствия
9	Удар молнии
10	Сильный снегопад
11	Сильные морозы
12	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обветшанием здания
13	Затопление водой в период паводка
14	Наводнение, вызванное проливным дождем
15	Ураган, торнадо
16	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод
	Телекоммуникационные и ИТ угрозы
17	Сбой системы кондиционирования
18	Сбой ИТ — систем
	Угроза, связанная с человеческим фактором
19	Ошибка персонала, имеющего доступ к серверной
20	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
	Угрозы, связанные с внешними поставщиками
21	Отключение электроэнергии
22	Сбой в работе интернет провайдера
23	Физически разрыв внешних каналов связи

Памятка по работе с корпоративной электронной почтой

Политика использования электронной почты является важнейшим элементом общекорпоративной политики информационной безопасности организации.

Электронная почта является собственностью Областного государственного казенного учреждения социального обслуживания «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска» (далее - учреждение) и может быть использована ТОЛЬКО в служебных целях. Использование электронной почты в других целях категорически запрещено.

Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

При работе с корпоративной системой электронной почты сотрудникам учреждения запрещается:

использовать адрес корпоративной почты для оформления подписок;

– публиковать свой адрес либо адреса других сотрудников учреждения на общедоступных Интернет-ресурсах (форумы, конференции и т.п.) за исключением случаев служебной необходимости;

– осуществлять массовую рассылку почтовых сообщений рекламного характера;

– 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, 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-либо было пароль доступа к своему почтовому ящику.

Ведущий системный администратор А.А. Лебедев

УТВЕРЖДАЮ
Директор ОГКУСО «Центр помощи
детям, оставшимся без попечения
родителей, г. Ангарска»
_____ Н.А. Олухова
«10» _____ 2024 г.

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Областного государственного казенного учреждения социального обслуживания «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска»

1. Общие положения.

1.1. Настоящее Положение разработано в целях защиты персональных данных, обрабатываемых в информационных системах персональных данных Областного государственного казенного учреждения социального обслуживания «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска» (далее - учреждение), от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Положение определяет обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных.

1.3. Положение разработано на основании ст. 24 Конституции РФ, Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006 г., Закона «Об информации, информатизации и защите информации» № 149- ФЗ от 27.07.2006 г., Постановления Правительства Российской Федерации от 01.11.2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативно-правовыми актами Российской Федерации в области трудовых отношений.

1.4. Настоящее Положение утверждается директором учреждения.

1.5. Изменения в Положение могут быть внесены в установленном действующим законодательством порядке.

1.6. В настоящем Положении используются следующие основные понятия:

1.6.1. Персональные данные (ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных) - работнику, служащему, государственному гражданскому служащему, заявителю на получение мер социальной поддержки, контрагенту.

1.6.2. Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

1.6.3. Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

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

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

права и свободы субъекта персональных данных или других лиц.

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

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

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

1.6.9. Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

1.6.10. 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.

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

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

2. Понятие и содержание персональных данных.

2.1. Персональные данные - информация, необходимая для осуществления основной деятельности учреждения и кадрового учета сотрудников.

2.2. Оператором персональных данных является учреждение.

2.3. Допускается привлекать для обработки персональных данных уполномоченные организации на основе соответствующих договоров и соглашений.

2.4. Персональные данные являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения, соответствующий гриф ограничения на них не ставится.

2.5. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания и в отношении общедоступных персональных данных.

3. Порядок получения и обработки персональных данных.

3.1. Получение персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений, защиты персональных данных, нормативными и распорядительными документами учреждения на основе согласия субъектов на обработку их

персональных данных.

3.2. Без согласия субъектов осуществляется обработка общедоступных персональных данных или содержащих только фамилии, имена и отчества, обращений и запросов организаций и физических лиц, регистрация и отправка корреспонденции почтовой связью, оформление разовых пропусков, обработка персональных данных для исполнения трудовых договоров или без использования средств автоматизации, и в иных случаях, предусмотренных законодательством Российской Федерации.

3.3. Обработка и использование персональных данных осуществляется в целях, указанных в соглашениях с субъектами персональных данных, а также в случаях, предусмотренных нормативно-правовыми актами Российской Федерации.

3.4. Не допускается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

3.5. В случае увольнения субъекта персональных данных и иного достижения целей обработки персональных данных, зафиксированных в письменном соглашении, Оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами.

3.6. Правила обработки и использования персональных данных устанавливаются отдельными регламентами и инструкциями учреждения.

3.7. Персональные данные могут храниться в бумажном и (или) электронном виде централизованно или в соответствующих структурных подразделениях с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации мер по защите персональных данных.

3.8. Перечень структурных подразделений и (или) отдельных должностей, имеющих право на обработку персональных данных, предоставляется работникам структурных подразделений и (или) должностным лицам, определенным отдельными Приказами, распорядительными документами и иными письменными указаниями уполномоченных сотрудников учреждения.

3.9. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты, информации, а также утвержденными регламентами и инструкциями Оператора

3.10. До начала осуществления трансграничной передачи персональных данных ответственный работник учреждения обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных.

3.11. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

3.11.1. Наличия согласия в письменной форме субъекта персональных данных.

3.11.2. Предусмотренных международными договорами

Российской Федерации по вопросам выдачи виз, международными договорами Российской Федерации об оказании правовой помощи по гражданским, семейным и уголовным делам, а также международными договорами Российской Федерации о ремиссии.

3.11.3. Предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства.

3.11.4. Исполнения договора, стороной которого является субъект персональных данных.

3.11.5. Защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

4. Права, обязанности и ответственность субъекта персональных данных и Оператора при обработке персональных данных.

4.1. В целях обеспечения защиты своих персональных данных субъект персональных данных в соответствии с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ «О персональных данных» за исключением случаев, предусмотренных данным Федеральным законом, имеет право:

4.1.1. На получение сведений об Операторе, о месте его нахождения, о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными.

4.1.2. Требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

4.1.3. На получение при обращении или при получении запроса информации, касающейся обработки его персональных данных.

4.1.4. На обжалование действий или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

4.1.5. На защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

4.2. Обязанности Оператора при сборе персональных данных.

4.2.1. Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

4.2.2. О внесенных изменениях и предпринятых мерах Оператор обязан уведомить субъекта персональных данных или его законного представителя и

третьих лиц, которым персональные данные этого субъекта были переданы.

4.2.3. В случае выявления неправомерных действий с персональными данными Оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения.

4.2.4. В случае невозможности устранения допущенных нарушений Оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные.

4.2.5. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя.

4.2.6. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Оператором и субъектом персональных данных.

4.2.7. Об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных.

4.3. Права Оператора на передачу персональных данных третьим лицам.

4.3.1. Оператор не вправе без письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации.

4.3.2. Передача персональных данных субъекта третьим лицам должна производится в соответствии с Регламентом передачи персональных данных третьим лицам.

5. Ответственность за разглашение персональных данных.

5.1. Оператор, а также должностные лица, виновные в нарушении требований Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

5.2. Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается в приказе об утверждении Положения и иных приказах на руководителей структурных подразделений и конкретных должностных лиц Оператора, обрабатывающих персональные данные.

6. Основные принципы построения системы комплексной защиты информации.

Построение системы обеспечения безопасности персональных данных информационных систем персональных данных учреждения и их функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;

- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

6.1 Законность

Предполагает осуществление защитных мероприятий и разработку системы защиты персональных данных (СЗПДн) учреждения в соответствии с действующим законодательством в области защиты персональных данных и других нормативных актов по защите информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал информационных систем персональных данных учреждения должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту персональных данных.

6.2 Системность

Системный подход к построению СЗПДн учреждения предполагает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ИСПДн учреждения.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки персональных данных, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределённые системы и несанкционированного доступа (далее - НСД) к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

6.3 Комплексность

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

6.4 Непрерывность защиты персональных данных

Защита персональных данных - непрерывный целенаправленный процесс,

предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационной системы персональных данных.

Информационные системы персональных данных должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода информационных систем персональных данных в незащищенное состояние.

6.5 Своевременность

Предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите информационных систем персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационных систем персональных данных в целом и ее системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы.

6.6 Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем персональных данных и их системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

6.7 Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

6.8 Принцип минимизации полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

Доступ к персональным данным должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

6.9 Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность информационных систем персональных учреждения, для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

6.10 Гибкость системы защиты персональных данных

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем

защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

6.11 Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

6.12 Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов информационной системы персональных данных.

6.13 Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности персональных данных.

Система защиты персональных данных должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

6.14 Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности персональных данных, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами учреждения.

6.15 Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности персональных данных на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

7. Меры, методы и средства обеспечения требуемого уровня защищённости.

Обеспечение требуемого уровня защищённости должности достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности информационных систем персональных данных подразделяются на:

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

Перечень выбранных мер обеспечения безопасности отражается в Плане мероприятий по обеспечению защиты персональных данных.

7.1 Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию персональных данных и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

7.2 Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

7.3 Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования информационных систем персональных данных, использование ресурсов информационных систем персональных данных, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с информационными системами персональных данных таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику информационной безопасности персональных данных (отражающую подходы к защите информации) и обеспечить

ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация политики информационной безопасности персональных данных в информационных системах персональных данных состоят из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность рассматриваемых в целом. Эти решения закрепляются в локальных актах учреждения. Примером таких решений могут быть:

- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности персональных данных, определение ответственных за ее реализацию;
- формулирование целей, постановка задач, определение направлений деятельности в области безопасности персональных данных;
- принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне учреждения в целом;
- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности персональных данных, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью информационных систем.

На организационном уровне определяются процедуры и правила достижения целей и решения задач политики информационной безопасности персональных данных. Эти правила определяют:

- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности персональных данных, а также их установить ответственность;
- кто имеет права доступа к персональным данным;
- какими мерами и средствами обеспечивается защита ПДн;
- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;
- определять коалиционные и иерархические принципы и методы разграничения доступа к персональным данным;
- определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;
- организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

В организационные меры должны состоять из:

- ограничение доступа в помещения, где расположены ИСПДн и их отдельные элементы;
- порядок допуска сотрудников к использованию ресурсов ИСПДн учреждения;
- регламента процессов ведения баз данных и осуществления модификации

информационных ресурсов;

- регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;

- инструкций пользователей ИСПДн (администратора, администратора безопасности, оператора);

7.4 Физические меры защиты

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

7.5 Аппаратно-программные средства защиты ПДн

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности ПДн и информационных системах по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;

- средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн учреждения;

- средства обеспечения и контроля целостности программных и информационных ресурсов;

- средства оперативного контроля и регистрации событий безопасности;

- криптографические средства защиты ПДн.

Успешное применение технических средств защиты на основании представленных выше принципов предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент ИСПДн;

- каждый сотрудник (пользователь) или группа пользователей ИСПДн имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

- все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются)

только на основании распоряжений руководства учреждения;

- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).

- специалистами учреждения осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

УТВЕРЖДАЮ
Директор ОГКУСО «Центр помощи детям, оставшимся без попечения родителей, г. Ангаска»
_____ Н.А. Олухова
«15» 10 2024 г.

ПОЛОЖЕНИЕ О ПОРЯДКЕ УЧЕТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Областного государственного казенного учреждения социального обслуживания «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска»

1. Общие положения

Настоящее Положение разработано в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», Федеральным законом № 152-ФЗ от 27.07.2006 г. «О персональных данных», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, и устанавливает порядок использования носителей информации, предоставляемых областного государственного казенного учреждения социального обслуживания «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска» (далее – учреждение) для использования в информационных системах персональных данных.

1.1. Действие настоящего Положения распространяется на сотрудников учреждения, подрядчиков и третью сторону.

2. Основные термины, сокращения и определения

Администратор ИСПДн — технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения и оборудования вычислительной техники.

АРМ - автоматизированное рабочее место пользователя (персональный компьютер, предназначенный для выполнения определенной производственной задачи).

ИБ - информационная безопасность - комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

ИСПДн- информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Носитель информации - любой материальный объект, используемый для хранения и передачи электронной информации.

Паспорт ПК - документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

ПК - персональный компьютер.

ПО - программное обеспечение вычислительной техники.

ПО вредоносное - ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

ПО коммерческое - ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

Пользователь — работник учреждения, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

3. Порядок использования носителей информации

3.1. Под использованием носителей информации в ИСПДн учреждения

понимается их подключение к инфраструктуре ИСПДн с целью обработки, приема/передачи информации между ИСПДн и носителями информации.

3.2. В ИСПДн допускается использование только учтенных носителей информации, которые являются собственностью учреждения и подвергаются регулярной ревизии и контролю.

3.3. К предоставленным учреждения носителям конфиденциальной информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИСПДн).

3.4. Носители конфиденциальной информации предоставляются сотрудникам учреждения по инициативе Руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника учреждения производственной необходимости.

3.5. Процесс предоставления сотрудникам учреждения носителей конфиденциальной информации (персональных данных) состоит из следующих этапов:

4. Порядок учета и хранения со съемными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации.

4.1. Все находящиеся на хранении и в обращении съемные носители с конфиденциальной информацией (персональными данными) в учреждении подлежат учёту.

4.2. Каждый съемный носитель с записанными на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу съемных носителей конфиденциальной информации (персональных данных) осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

4.4. Сотрудники учреждения получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

5. При использовании сотрудниками носителей конфиденциальной информации (персональных данных) необходимо:

5.1. Соблюдать требования настоящего Положения.

5.2. Использовать носители информации исключительно для выполнения своих служебных обязанностей.

5.3. Ставить в известность администраторов ИСПДн о любых фактах

нарушения требований настоящего Положения.

5.4. Бережно относится к носителям конфиденциальной информации (персональных данных).

5.5. Обеспечивать физическую безопасность носителей информации всеми разумными способами.

5.6. Извещать администраторов ИСПДн о фактах утраты (кражи) носителей конфиденциальной информации (персональных данных).

6. При использовании носителей конфиденциальной информации (персональных данных) запрещено:

6.1. Использовать носители конфиденциальной информации (персональных данных) в личных целях.

6.2. Передавать носители конфиденциальной информации (персональных данных) другим лицам (за исключением администраторов ИСПДн).

6.3. Хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

6.4. Выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

7. Порядок обращения со съемными носителями конфиденциальной информации (персональных данных)

7.1. Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником учреждения между ИСПДн и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с администраторами ИСПДн заранее). Администратор ИСПДн оставляет за собой право блокировать или ограничивать использование носителей информации.

7.2. Информация об использовании сотрудником учреждения носителей информации в ИСПДн протоколируется и, при необходимости, может быть предоставлена руководителям структурных подразделений, а также начальнику управления информационной безопасности и межведомственного взаимодействия.

7.3. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей конфиденциальной информации (персональных данных) инициализируется служебная проверка, проводимая комиссией, состав которой определяется ведущим системным администратором учреждения.

7.4. По факту выясненных обстоятельств составляется акт расследования инцидента и передается Руководителю структурного подразделения для принятия мер согласно локальным нормативным актам учреждения и действующему законодательству.

7.5. Информация, хранящаяся на носителях конфиденциальной информации (персональных данных), подлежит обязательной проверке на

отсутствие вредоносного ПО.

7.6. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

7.7. Вынос съемных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

7.8. В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

7.9. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт по прилагаемой форме

7.10. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители конфиденциальной информации изымаются.

8. Ответственность

8.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами учреждения.

УТВЕРЖДАЮ
Директор ОГКУСО «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска»
_____ Н.А. Олухова
«15» 10 2024 г.

РЕГЛАМЕНТ ИСПЛЬЗОВАНИЯ РЕСУРСОВ ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ

Областного государственного казенного учреждения социального обслуживания «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска»

1. Общие положения

Настоящий Регламент разработан для повышения эффективности работы сотрудников Областного государственного казенного учреждения социального обслуживания «Центр помощи детям, оставшимся без попечения родителей, г. Ангарска» (далее – учреждение), использующих электронные информационные ресурсы глобальной сети Интернет, и повышения уровня информационной безопасности локальной информационно-вычислительной сети учреждения.

В учреждении устанавливается контроль, и специфицируются виды информации, к которой разрешается доступ сотрудников. В случае нарушения сотрудником учреждения данного Регламента он отстраняется от использования ресурсов сети Интернет.

2. Назначение доступа к ресурсам сети Интернет

Доступ к ресурсам сети Интернет предоставляется сотрудникам учреждения для выполнения ими прямых должностных обязанностей. Глобальная сеть Интернет используется для:

- доступа к гипертекстовым страницам (WWW);
- доступа к файловым ресурсам Интернета (FTP);
- доступа к специализированным (правовым и др.) базам данных;
- ответов на официальные запросы граждан;
- обмена электронной почтой с официальными лицами других правительственных структур по не конфиденциальным вопросам производственного характера;
- повышения квалификации работников, необходимой для выполнения работником своих должностных обязанностей;
- поиска и сбора информации по управленческим, производственным, финансовым, юридическим вопросам, если эти вопросы напрямую связаны с выполнением работником его должностных обязанностей, и др.

3. Доступ к Интернет-ресурсам

Учреждение обеспечивает доступ пользователей локальной сети, к ресурсам Интернет по специальным каналам связи в соответствии с установленными в учреждении правилами и настоящим Регламентом.

Открытие и контроль доступа регулируется управлением информационной безопасности и межведомственного взаимодействия учреждения. Самостоятельная организация дополнительных точек доступа в глобальную сеть Интернет (удаленный доступ, VPN и пр.) запрещена.

4. Регистрация пользователя

Каждому физически подключенному к сети компьютеру назначается ответственный за этот компьютер пользователь, информация о котором заносится в базу данных пользователей соответствующего домена локальной сети учреждения.

Регистрация выполняется системным администратором на основании приказа руководителя подразделения. Пользователь обязан хранить свои идентификационные данные (пароли и т.п.) в тайне. Запрещена передача идентификационных данных третьим лицам. За все деструктивные действия, произведенные в сети, отвечает сотрудник - пользователь учетной записи (идентификационных данных), использовавшейся при их проведении.

При подозрении на то, что идентификационные данные стали известны третьим

лицам, пользователь должен немедленно обратиться к ведущему системному администратору учреждения с целью их изменения.

5. Основные ограничения при работе в сети Интернет

При работе в сети Интернет запрещается:

- посещение пользователем ресурсов с непристойным содержанием (эротико-порнографические ресурсы, нацистские или националистические ресурсы, ресурсы, призывающие к насилию);

посещение игровых, развлекательных и прочих сайтов, не имеющих отношения к деятельности учреждения и деятельности пользователя;

- использование электронной почты в личных целях в любое время;
- массовая рассылка не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю. Здесь и далее под электронными письмами понимаются сообщения электронной почты, ICQ и других подобных средств личного обмена информацией;
- несогласованная рассылка электронных писем рекламного, коммерческого или агитационного характера, а также писем, содержащих грубые и оскорбительные выражения и предложения;
- использование собственных или предоставленных информационных ресурсов (почтовых ящиков, адресов электронной почты, страниц WWW и т.д.) в качестве контактных для осуществления действий, не связанных с выполнением служебных обязанностей;
- не допускается осуществление попыток несанкционированного доступа к ресурсам Сети, проведение или участие в сетевых атаках и сетевом взломе, за исключением случаев, когда атака на сетевой ресурс проводится с явного разрешения владельца или администратора этого ресурса;
- действия, направленные на нарушение нормального функционирования элементов Сети (компьютеров, другого оборудования или программного обеспечения), не принадлежащих пользователю;
- передача компьютерам или оборудованию Сети информации, не имеющей отношения к выполнению служебных обязанностей, создающей паразитную нагрузку на рабочие станции локальной сети и (или) оборудование, а также промежуточные участки сети, в объемах, превышающих минимально необходимые для проверки связности сетей и доступности отдельных ее элементов.
- публикация корпоративного электронного адреса @ на досках объявлений, в конференциях и гостевых книгах;
- использование некорпоративных E-mail.
- передача кому бы то ни было учетных данных пользователя;

применение имен и паролей учетных записей, используемых в локальной сети учреждения, на иных (сторонних) компьютерах;

установка и использование сетевых и автономных компьютерных игровых приложений на рабочей станции;

- посещение ресурсов трансляции потокового видео и аудио (вебкамеры, трансляция ТВ - и музыкальных программ в Интернете), создающих большую загрузку сети и мешающих нормальной работе остальных пользователей;
- загрузка развлекательных материалов;
- передача конфиденциальной информации третьей стороне;
- подключение к электронной сети под чужим логином и паролем;
- нанесение вреда электронной системе учреждения;
- проведение незаконных операций в глобальной сети Интернет;

создание личных веб-страниц и хостинг (размещение web- или ftp- сервера) на рабочих станциях локальной вычислительной сети учреждения;

- любые попытки деструктивных действий по отношению к нормальной работе электронной системы учреждения и ресурсам сети Интернет (рассылка вирусов, ip-атаки и т.п.);
- нарушение закона об авторском праве: копирование и использование материалов и программ, защищенных законом об авторском праве;
- совершение иных действий, противоречащих действующему законодательству Российской Федерации.

6. Соблюдение правил, установленных владельцами ресурсов.

Владелец любого информационного или технического ресурса сети Интернет может установить для этого ресурса собственные правила его использования. Правила использования ресурсов либо ссылка на них публикуются владельцами или администраторами этих ресурсов в точке подключения к таким ресурсам и являются обязательными к исполнению всеми пользователями этих ресурсов. Пользователь обязан соблюдать правила использования ресурса либо немедленно отказаться от его использования.

7. Недопустимость фальсификации.

Значительная часть ресурсов Сети не требует идентификации пользователя и допускает анонимное использование. Однако в ряде случаев от пользователя требуется предоставить информацию, идентифицирующую его, и используемые им средства доступа к Сети. При этом пользователю запрещается:

- использование идентификационных данных (имен, адресов, телефонов и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование. В то же время пользователь должен принять меры по предотвращению использования ресурсов Сети третьими лицами от его имени (обеспечить сохранность паролей и прочих кодов авторизованного доступа);
- фальсификация своего IP-адреса, а также адресов, используемых в других сетевых протоколах, при передаче данных в Сеть;
- использование несуществующих обратных адресов при отправке электронных писем.

Ответственность за все действия в Сети, произведенные под именем и с паролем пользователя им самим или другими физическими, или юридическими лицами и организациями, полностью лежит на самом пользователе. Учреждение не несет никакой юридической, материальной или иной ответственности за качество, содержание, законность и любое другое свойство полученной или переданной пользователем информации в нарушение действующего законодательства Российской Федерации.

Учреждение не несет никакой юридической, материальной и иной ответственности за использование пользователем платных услуг других организаций, предоставляющих услуги в Сети.

8. Контроль использования ресурсов сети Интернет

Руководство учреждения оставляет за собой право в целях обеспечения безопасности электронной системы производить выборочные и полные проверки всей электронной системы и отдельных файлов без предварительного уведомления работников.