УТВЕРЖДАЮ
Директор ГБУ СОН АО «Коношский КЦСО»
_____ Е.Е. Золотых
«9» января 2023 г.

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГБУ СОН АО «Коношский КЦСО»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГБУ СОН АО «Коношский КЦСО» (далее – Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Цель разработки настоящего Положения – установление порядка организации и проведения работ по обеспечению безопасности персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн) ГБУ СОН АО «Коношский КЦСО» (далее – Коношский КЦСО) на протяжении всего жизненного цикла ИСПДн.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания, если иное не предусмотрено федеральным законом.

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

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

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), 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 и обработке в ИСПДн понимается формирование и реализация совокупност согласованных по цели, задачам, месту и времени организационных технических мероприятий, направленных на минимизацию ущерба о возможной реализации угроз безопасности ПДн, реализуемых в рамка создаваемой системы защиты персональных данных (далее – СЗПДн).

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

3.3. Безопасность ПДн при их обработке в ИСПДн обеспечивае Коношский КЦСО или лицо, осуществляющее обработку ПДн по поручени Коношского КЦСО на основании заключаемого с этим лицом договор (далее – уполномоченное лицо). Договор между Коношским КЦСО уполномоченным лицом должен предусматривать обязанност уполномоченного лица обеспечить безопасность ПДн при их обработке информационной системе.

3.4. Выбор средств защиты информации для СЗПДн осуществляетс Коношским КЦСО в соответствии с нормативными правовыми актам принятыми Федеральной службой безопасности Российской Федераци (далее – ФСБ России) и Федеральной службой по техническому экспортному контролю (далее – ФСТЭК России) во исполнени Федерального закона «О персональных данных».

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

3.6. СЗПДн создается в три этапа:

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

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

Этап 3. Ввод ИСПДн с СЗПДн в эксплуатацию.

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

3.7.1. Назначение ответственного за организацию обработки ПД Коношским КЦСО.

3.7.2. Создание комиссии по определению уровня защищенност ПДн при их обработке в ИСПДн Коношского КЦСО.

3.7.3. Определение целей обработки ПДн Коношским КЦСО.

3.7.4. Определение перечня ИСПДн Коношского КЦСО и состава ПДн, обрабатываемых в ИСПДн.

3.7.5. Определение перечня обрабатываемых Коношским КЦСО ПДн.

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

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

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

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

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

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

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

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

3.7.14. Формирование технических паспортов ИСПДн.

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

– Политика в отношении обработки персональных данных;

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

– Раздел должностных инструкций сотрудников Коношского КЦСО в части обеспечения безопасности ПДн при их обработке, включая

установление персональной ответственности за нарушения правил обработк ПДн.

3.7.16. Получение (при необходимости) согласия на обработку ПД субъектом ПДн, подписание обязательства о соблюдени конфиденциальности ПДн сотрудниками Коношского КЦСО.

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

3.7.18. Определение уровня защищенности ПДн при их обработке ИСПДн в соответствии с требованиями постановления Правительств Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждени требований к защите персональных данных при их обработке информационных системах персональных данных» (подготовка утверждение акта определения уровня защищенности ПДн при их обработ в ИСПДн).

3.7.19. Определение типа угроз безопасности ПДн, актуальных дл информационной системы, с учетом оценки возможного вреда соответствии с нормативными правовыми актами, принятыми во исполнени Федерального закона «О персональных данных» от 27 июля 2006 г. № 15 Определение угроз безопасности ПДн в конкретных условия функционирования ИСПДн (разработка моделей угроз безопасности ПД при их обработке в ИСПДн).

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

Техническое задание на разработку СЗПДн должно содержать:

– обоснование разработки СЗПДн;

– исходные данные создаваемой (модернизируемой) ИСПДн техническом, программном, информационном и организационном аспектах;

– уровень защищенности ПДн при их обработке в ИСПДн;

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

– конкретизацию мероприятий и требований к СЗПДн;

– состав и содержание работ по этапам разработки и внедрения СЗПД

– перечень предполагаемых к использованию сертифицированны средств защиты информации.

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

3.8.1. Создание СЗПДн является необходимым услови

обеспечения безопасности ПДн, в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиям к обеспечению безопасности ПДн для соответствующего уровня защищенности ПДн при их обработке в ИСПДн и (или) не нейтрализуют всех угроз безопасности ПДн для данной ИСПДн.

3.8.2. Технические меры защиты ПДн предполагают использование программно-аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов Коношского КЦСО. Применение технических мер должно быть регламентировано локальным актом Коношского КЦСО.

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

3.8.4. На стадии проектирования и создания СЗПДн для ИСПДн Коношского КЦСО проводятся следующие мероприятия:

– разработка технического проекта СЗПДн;

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

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

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

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

– подготовка эксплуатационной документации на используемые средства защиты информации;

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

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

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

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

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

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

3.9.2. Контроль за выполнением настоящих требований организуется и проводится Коношским КЦСО (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 Коношским КЦСО (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 обработки и защиты ПДн Коношским КЦСО проводятся в соответствии с Планом внутренних проверок режима обработки и защиты персональных данных (ПРИЛОЖЕНИЕ № 2). По результатам проведения внутренней проверки составляется Отчет о результатах проведения внутренней проверки режима обработки и защиты персональных данных в ГБУ СОН АО «Коношский КЦСО» (ПРИЛОЖЕНИЕ № 3).

4.2. Контроль за проведением работ по обеспечению безопасности ПДн осуществляет ответственный за организацию обработки ПДн в виде методического руководства, участия в разработке требований по защите ПДн, организации работ по выявлению возможных каналов утечки информации, согласования выбора средств вычислительной техники и связи, технических и программных средств защиты, участия в оценке соответствия ИСПДн Коношского КЦСО 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 Постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных

использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», при необходимости использования при создании СЗПДн средств криптографической защиты информации к проведению работ по обеспечению безопасности ПДн Коношскому КЦСО 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. ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ КОНОШСКОГО КЦСО

5.1. Настоящий порядок определяет правила проведения резервного копирования данных, обрабатываемых в ИСПДн Коношского КЦСО.

5.2. Целью резервного копирования является предотвращение потери информации при сбоях оборудования, программного обеспечения, в критических и кризисных ситуациях и т.д.

5.3. Резервному копированию подлежит информация, обрабатываемая в ИСПДн Коношского КЦСО.

5.4. В Коношском КЦСО должна быть реализована централизованная система резервного копирования.

5.5. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации в установленные сроки и с заданной периодичностью.

5.6. Перед выполнением процедур резервного копирования и
восстановления информации и программного обеспечения средств защит
необходимо провести проверку:

– доступности резервного носителя, достаточности свободного места
хранилище для записи или восстановления данных;

– работоспособности средств резервного копирования
восстановления;

– готовности информационных ресурсов к осуществлению
резервного копирования или восстановления;

– завершения работы ПО и процессов, способных повлиять на проце
создания или восстановления копий.

5.7. Расписание проведения резервного копирования определяет
Ответственным.

5.8. Резервное копирование проводится Ответственным
регистрируется в Журнале резервного копирования и восстановлен
информации (ПРИЛОЖЕНИЕ № 4).

5.9. Перечень информационных ресурсов, подлежащих резервно
копированию, время и дата создания копии, пометки
успешном/неуспешном завершении, а также, при необходимост
комментарии Ответственного заносятся в Журнал резервного копирования
восстановления информации.

5.10.В случае выявления нарушений Ответственному необходимо
кратчайшие сроки устранить неисправности в системе резервно
копирования и восстановить работоспособность подсистем в штатный реж
работы.

5.11.О выявленных попытках несанкционированного доступа
резервируемой информации, а также иных нарушениях информационн
безопасности, произошедших в процессе резервного копирован
Ответственный сообщает руководству Коношского КЦСО немедленно.

5.12.Ответственный должен контролировать проведение резервно
копирования в целях выполнения требований по защите информации.

5.13.В случае обнаружения ошибки резервного копирован
Ответственный выполняет повторное копирование информации вручную
максимально сжатые сроки, не нарушая технологические процес
обработки информации пользователями Коношского КЦСО, в Журн
резервного копирования и восстановления информации занося
соответствующие отметки.

5.14.Хранение резервных копий данных осуществляется на сменн
носителях информации (CD/DVD, внешние жесткие диски и т.

промаркированных Ответственным в соответствии с расписанием резервного копирования. Маркировка должна содержать номер копии, дату ее создания, наименование ИСПДн.

5.15.Использование носителей информации при резервном хранении должно подчиняться принципу ротации носителей, при котором для записи текущей копии используется носитель с самой ранней датой создания предыдущей копии.

5.16.Срок хранения резервных копий определяется Ответственным.

5.17.Очистка устаревших резервных копий из хранилища должна производиться Ответственным регулярно по мере заполнения выделенной области памяти или по истечении предусмотренного срока хранения.

5.18.Удаление резервных копий для повторного использования носителя информации либо окончательное удаление производится Ответственным.

5.19.Основанием для инициирования процедуры восстановления служит полная или частичная утрата информации вследствие сбоев оборудования, программного обеспечения, в критических и кризисных ситуациях. Восстановление данных производится Ответственным.

5.20.Восстановление утраченных данных производится из резервной копии, обеспечивающей минимальную потерю данных, содержащихся в информационном ресурсе.

5.21.В зависимости от характера и уровня повреждения информационных ресурсов, Ответственный восстанавливает либо весь архив копии данных, либо отдельные потерянные части или технические средства из соответствующих хранилищ.

5.22.После завершения процесса восстановления Ответственным проверяется целостность информационных ресурсов и корректная работа технических средств информационных систем, также заполняются соответствующие поля в Журнале резервного копирования и восстановления информации.

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

6.1. Модернизация СЗПДн для функционирующих ИСПДн Коношского КЦСО должна осуществляться в случае:

– изменения состава или структуры ИСПДн или технических особенностей ее построения (изменения состава или структуры

программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);

– изменения состава угроз безопасности ПДн в ИСПДн;

– изменения уровня защищенности ПДн при их обработке в ИСПДн;

– прочих случаях, по решению Коношского КЦСО.

6.2. В целях определения необходимости доработки (модернизации СЗПДн не реже одного раза в год ответственным за организацию обработки ПДн должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и уровня защищенности ПДн при их обработке в ИСПДн, соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Результаты проверки оформляются актом проверки и утверждаются руководителем Коношского КЦСО.

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

– несоблюдение условий хранения носителей ПДн;

– использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн;

– нарушение заданного уровня безопасности ПДн (конфиденциальность/ целостность/доступность).

ПРИЛОЖЕНИЕ № 1
к Положению по организации и
проведению работ по обеспечению
безопасности персональных данных
при их обработке в информационных
системах персональных данных ГБУ
СОН АО «Коношский КЦСО»
от «9» января 2023 г.

План мероприятий по защите персональных данных
в ГБУ СОН АО «Коношский КЦСО»

№ 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	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствие с требованиями закона необходимо разграничить доступ

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
		ИСПДн)	сотрудников Коношского Кцсо к ПДн
5.	Взаимодействие с субъектами ПДн	Постоянно	Работа с обращениями субъектов ПДн, ведение журналов учета передач 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 электронных носителей персональных данных, средств защиты информации	Постоянно	
7.	Повышение квалификации сотрудников в области защиты ПДн	Постоянно	Повышение квалификации сотрудников, ответственных за выполнение работ – не менее раза в три года, повышение осведомленности сотрудников постоянно (данное обучение проводит ответственный за обеспечение безопасности ПДн в ИСПДн)
8.	Инвентаризация информационных ресурсов	Раз в полгода	Проводится с целью выявления в информационных ресурсах присутствия ПДн
9.	Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки	При необходимости	Для уничтожения ПДн Коношского КЦСО устанавливаются сроки обработки ПДн, которые документально подтверждаются в локальных актах Коношского КЦСО. 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 «О комиссии по уничтожению персональных данных»
11.	Определение уровня защищенности ПДн при их обработке в ИСПДн	При необходимости	Определение уровня защищенности ПДн при их обработке в ИСПДн осуществляется при создании ИСПДн, при изменении состава ПДн, объема обрабатываемых ПДн, субъектов ПДн
12.	*Выявление угроз безопасности* и разработка моделей угроз и нарушителя	При необходимости	Разрабатывается при создании системы защиты ИСПДн
13.	Аттестация ИСПДн на соответствие требованиям по обеспечению безопасности ПДн	При необходимости	Проводится совместно с лицензиатом ФСТЭК
14.	Эксплуатация ИСПДн и контроль безопасности ПДн	Постоянно	
15.	Понижение требований по	При	В случае создания ИСПДн, а. та

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
	защите ПДн путем сегментирования ИСПДн, отключения от сетей общего пользования, обеспечения обмена между ИСПДн с помощью сменных носителей, создания автономных ИСПДн на выделенных АРМ и прочих доступных мер	необходимости	приведения имеющихся ИСПДн в соответствии с требованиями закона

ПРИЛОЖЕНИЕ № 2
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГБУ СОН АО «Коношский КЦСО»
от «9» января 2023 г.

План внутренних проверок режима обработки и защиты персональных данных в ГБУ СОН АО «Коношский КЦСО»

№	Мероприятие	Периодичность	Дата, подпис исполнител
1.	Осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн ФЗ-152 «О персональных данных» и принятым в соответствии с ним нормативным правовым актам	Раз в полгода	
2.	Проверка ознакомления сотрудников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн	Раз в полгода	
3.	Проверка получения согласий субъектов ПДн на обработку ПДн в случаях, когда этого требует законодательство	Раз в полгода	
4.	Проверка подписания сотрудниками, осуществляющими обработку ПДн, основных форм, необходимых в целях выполнения требований законодательства в сфере обработки и защиты ПДн: - Уведомления о факте обработки ПДн без использования средств автоматизации; - Обязательства о соблюдении конфиденциальности ПДн; - Формы ознакомления с положениями законодательства Российской Федерации о ПДн, локальными актами ГБУ СОН АО «Коношский КЦСО» по вопросам обработки ПДн; - Разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн	Раз в полгода	
5.	Проверка уничтожения материальных носителей ПДн с составлением соответствующего акта	Ежегодно	
6.	Проверка ведения журналов по учету обращений субъектов ПДн и учету передачи ПДн субъектов третьим лицам	Раз в полгода	
7.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн	Ежегодно	
8.	Проверка соблюдения условий хранения материальных носителей ПДн	Раз в полгода	
9.	Проверка состояния актуальности Уведомления об	Раз в полгода	

№	Мероприятие	Периодичность	Дата, подпись исполнителя
	обработке (намерении осуществлять обработку) ПДн		
10.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПДн, в том числе документов, определяющих политику ГБУ СОН АО «Коношский КЦСО» в отношении обработки ПДн	Раз в полгода	
11.	Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	
12.	Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ-152 «О персональных данных»	Ежегодно	
13.	Проверка применения для обеспечения безопасности ПДн средств защиты информации, прошедших в установленном порядке процедуру соответствия	Раз в полгода	
14.	Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн	При необходимости	
15.	Контроль учета машинных носителей ПДн	Раз в полгода	
16.	Контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ПДн в ИСПДн	Раз в полгода	
17.	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИСПДн	Ежеквартально	
18.	Контроль внесения изменений в структурно-функциональные характеристики ИСПДн	Ежеквартально	
19.	Контроль корректности настроек средств защиты информации	Раз в полгода	
20.	Контроль за обеспечением резервного копирования	Ежеквартально	
21.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам защиты ПДн	Раз в полгода	

ПРИЛОЖЕНИЕ № 3
к Положению по организации и
проведению работ по обеспечению
безопасности персональных данных при
их обработке в информационных системах
персональных данных ГБУ СОН АО
«Коношский КЦСО»
от «9» января 2023 г.

Отчет о результатах проведения внутренней проверки режима обработки и защиты персональных данных в ГБУ СОН АО «Коношский КЦСО»

1.1 Внутренняя проверка произведена на основании Положения по организации проведению работ по обеспечению безопасности персональных данных при их обработке информационных системах персональных данных ГБУ СОН АО «Коношский КЦСО» от «_ _____20__г.

1.2 Проверка проводилась «___»_____20__ г. по адресу:
_____
_____

1.3 В ходе проверки были проведены следующие мероприятия:
1) _____
2) _____
3) _____
4) _____
5) _____

1.4 Результаты проведения проверки:
1) _____
2) _____
3) _____
4) _____
5) _____

1.5 Необходимые мероприятия.
На основании проведения внутренней проверки режима обработки и защиты П рекомендуется осуществить следующие мероприятия:
1) _____
2) _____
3) _____
4) _____
5) _____

Подписи ответственных лиц, проводивших внутреннюю проверку режима обработки и защит ПДн:

_____ (дата)	_____ (подпись)	_____ (расшифровка подписи)
_____ (дата)	_____ (подпись)	_____ (расшифровка подписи)
_____ (дата)	_____ (подпись)	_____ (расшифровка подписи)

Приложение 1
к Положению по организации и
проведению работ по обеспечению
безопасности персональных данных
при их обработке в информационных
системах персональных данных ГБУ
СОН АО «Коношский КЦСО»
от «9» января 2023 г.

Журнал резервного копирования/восстановления данных

№ п/п	Схема резервного копирования/восстановления данных	Копируемые/восстанавливаемые ресурсы	Хранилище	Дата/время создания копии/восстановления	Фамилия ответственного	Подпись ответственного	Результат резервного копирования/восстановления данных	Комментарий
1	2	3	4	5	6	7	8	9