

УТВЕРЖДАЮ

Глава администрации Яльчикского
района Чувашской Республики

Н.П. Миллин

2016 г.



ПОЛОЖЕНИЕ

по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Яльчикского района Чувашской Республики

І. Общие положения

1.1 Настоящее Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Яльчикского района Чувашской Республики (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 21 марта 2012 № 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», 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 Составы 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) Администрации Яльчикского района Чувашской Республики (далее – Администрация района) на протяжении всего жизненного цикла ИСПДн.

II. 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.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

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).

III. Порядок организации и проведения работ по обеспечению безопасности персональных данных

3.1 Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз

безопасности ПДн, реализуемых в рамках создаваемой системы защиты персональных данных (далее - СЗПДн).

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

3.3 Безопасность ПДн при их обработке в ИСПДн обеспечивает оператор или лицо, осуществляющее обработку персональных данных 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 персональных данных при их обработке в информационной системе.

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

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

3.6 СЗПДн создается в три этапа:

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

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

Этап 3. Ввод ИСПДн с СЗПДн в эксплуатацию.

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

3.7.1. Назначение распоряжением главы администрации Яльчикского района Чувашской Республики ответственного за организацию обработки ПДн.

3.7.2. Создание в Администрации района комиссии по классификации ИСПДн и определению уровня защищенности ПДн при их обработке в ИСПДн.

3.7.3. Определение перечня субъектов персональных данных (физических лиц), ПДн которых обрабатываются в Администрации района, перечня обрабатываемых ПДн и перечня документов, содержащих ПДн.

3.7.4. Определение перечня ИСПДн в Администрации района и состава ПДн, обрабатываемых в ИСПДн. Перечень ИСПДн и обрабатываемых ПДн утверждается распоряжением главы администрации Яльчикского района Чувашской Республики.

3.7.5. Определение целей обработки персональных данных – выполнение требований трудового законодательства Российской Федерации и законодательства

о муниципальной службе в Российской Федерации, предоставление государственных и муниципальных услуг, выполнение возложенных на Администрацию района функций, полномочий и обязанностей, рассмотрение обращений граждан.

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 распоряжением главы администрации Яльчикского района Чувашской Республики ответственного за обеспечение безопасности ПДн в ИСПДн (далее - Ответственный) для разработки и осуществления технических мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн. Для каждой ИСПДн может быть назначен отдельный Ответственный.

3.7.10. Разработка разрешительной системы доступа (матрицы доступа) пользователей ИСПДн к обрабатываемой на ИСПДн информации.

3.7.11. Определение границ контролируемых зон путем издания соответствующего распоряжения главы администрации Яльчикского района Чувашской Республики и условий расположения ИСПДн относительно границ контролируемых зон.

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 следующих организационно-распорядительных документов (далее - ОРД), регламентирующих процесс обработки и защиты персональных данных:

- Положение о защите персональных данных;
- Инструкция ответственного за обеспечение безопасности ПДн в ИСПДн;
- Инструкция пользователя ИСПДн;
- Раздел должностных инструкций сотрудников Администрации района в части обеспечения безопасности ПДн при их обработке, включая установление персональной ответственности за нарушения правил обработки ПДн.

3.7.16. Классификация ИСПДн в соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008

№ 55/86/20 (подготовка и утверждение акта классификации).

3.7.17. Определение уровня защищенности ПДн при их обработке в ИСПДн в соответствии с «Требованиями к защите ПДн при их обработке в информационных системах персональных данных», утвержденными Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 (подготовка и утверждение акта определения уровня защищенности ПДн при их обработке в ИСПДн).

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

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

Техническое задание на разработку СЗПДн должно содержать:

- обоснование разработки СЗПДн;
- исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;
- уровень защищенности ПДн при их обработке в ИСПДн;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн, и приниматься в эксплуатацию ИСПДн;
- конкретизацию мероприятий и требований к СЗПДн;
- состав и содержание работ по этапам разработки и внедрения СЗПДн
- перечень предполагаемых к использованию сертифицированных средств защиты информации.

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

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

3.8.2. Технические меры защиты ПДн предполагают использование программно-аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в

процессе предпроектного обследования информационных ресурсов Администрации района. Применение технических мер должно быть регламентировано нормативным актом Администрации района.

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 Администрации района 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 (положений, приказов, паспортов ИСПДн, топологических схем, инструкций и других документов).

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 персональных данных).

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).

IV. 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 в Администрации района проводятся в соответствии с Планом внутренних проверок режима защиты персональных данных (Приложение № 2). Планы утверждаются главой администрации Яльчикского района Чувашской Республики

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 персональных данных, 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 Администрации района требованиям безопасности ПДн.

4.3. При необходимости к проведению работ по обеспечению безопасности персональных данных 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 21.02.2008 № 149/54-144, при необходимости использования при создании СЗПДн средств криптографической защиты информации к проведению работ по обеспечению безопасности персональных данных Администрации района 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.

V. Решение вопросов обеспечения безопасности персональных данных в динамике изменения обстановки и контроля эффективности защиты

5.1. Модернизация СЗПДн для функционирующих ИСПДн Администрации района должна осуществляться в случае:

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

- изменения состава угроз безопасности ПДн в ИСПДн;
- изменения уровня защищенности ПДн при их обработке в ИСПДн;
- прочих случаях, по решению оператора.

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

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

- несоблюдение условий хранения носителей персональных данных;
- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных;
- 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 Администрации Яльчикского района Чувашской Республики от «26» мая 2016 г.

План мероприятий по защите персональных данных в Администрации Яльчикского района Чувашской Республики

№ п/п	Наименование мероприятия	Срок выполнения	Дата	Ответственный	Примечание
1.	Документальное регламентирование работы с ПДн	При необходимости		Ответственный за организацию обработки персональных данных (Управляющий делами – начальник отдела организационной работы)	Разработка организационно-распорядительных документов по защите ПДн, либо внесение изменений в существующие
2.	Получение письменных согласий субъектов ПДн (физических лиц) на обработку ПДн в случаях, когда этого требует законодательство	Постоянно		Ответственный за организацию обработки персональных данных (Управляющий делами – начальник отдела организационной работы)	Письменное согласие получается при передаче ПДн субъектами для обработки в ИСПДн, либо для обработки без использования средств автоматизации. Форма согласия приведена в Положении о защите ПДн
3.	Пересмотр договора с субъектами ПДн в части обработки ПДн	При необходимости		Ответственный за организацию обработки персональных данных (Управляющий делами – начальник отдела организационной работы)	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствие с требованиями закона (например, в договор может быть включено согласие субъекта на обработку и передачу его ПДн). Пересмотр договоров проводится при необходимости и оставляется на усмотрение финансового отдела - оператора ПДн
4.	Ограничение доступа сотрудников к ПДн	При необходимости (при создании)		Ответственный за обеспечение безопасности персональных данных в информационных системах	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствие с требованиями закона

Приложение № 1

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Яльчикского района Чувашской Республики от «26» мая 2016 г.

План мероприятий по защите персональных данных в Администрации Яльчикского района Чувашской Республики

№ п/п	Наименование мероприятия	Срок выполнения	Дата	Ответственный	Примечание
1.	Документальное регламентирование работы с ПДн	При необходимости		Ответственный за организацию обработки персональных данных (Управляющий делами – начальник отдела организационной работы)	Разработка организационно-распорядительных документов по защите ПДн, либо внесение изменений в существующие
2.	Получение письменных согласий субъектов ПДн (физических лиц) на обработку ПДн в случаях, когда этого требует законодательство	Постоянно		Ответственный за организацию обработки персональных данных (Управляющий делами – начальник отдела организационной работы)	Письменное согласие получается при передаче ПДн субъектами для обработки в ИСПДн, либо для обработки без использования средств автоматизации. Форма согласия приведена в Положении о защите ПДн
3.	Пересмотр договора с субъектами ПДн в части обработки ПДн	При необходимости		Ответственный за организацию обработки персональных данных (Управляющий делами – начальник отдела организационной работы)	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствие с требованиями закона (например, в договор может быть включено согласие субъекта на обработку и передачу его ПДн). Пересмотр договоров проводится при необходимости и оставляется на усмотрение финансового отдела - оператора ПДн
4.	Ограничение доступа сотрудников к ПДн	При необходимости (при создании)		Ответственный за обеспечение безопасности персональных данных в информационных системах	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствие с требованиями закона

№ п/п	Наименование мероприятия	Срок выполнения	Дата	Ответственный	Примечание
		ИСПДн)		персональных данных (Главный специалист эксперт отдела культуры и информационного обеспечения)	необходимо разграничить доступ сотрудников финансового отдела к ПДн
5.	Взаимодействие с субъектами ПДн	Постоянно		Ответственный за организацию обработки персональных данных (Управляющий делами – начальник отдела организационной работы)	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 отчуждаемых электронных носителей персональных данных, средств защиты информации	Постоянно		Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (Главный специалист эксперт отдела культуры и информационного обеспечения)	
7.	Повышение квалификации сотрудников в области защиты ПДн	Постоянно		Ответственный за организацию обработки персональных данных (Управляющий делами – начальник отдела организационной работы)	Повышение квалификации сотрудников, ответственных за выполнение работ - не менее раза в три года, повышение осведомленности сотрудников - постоянно (данное обучение проводит ответственный за организации защиты ПДн)
8.	Инвентаризация информационных ресурсов	Раз в полгода		Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (Главный специалист эксперт отдела культуры и информационного обеспечения)	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 каждой ИСПДн организацией - оператором ПДн должны быть установлены сроки обработки ПДн, что должно быть документально подтверждено в Положении

№ п/п	Наименование мероприятия	Срок выполнения	Дата	Ответственный	Примечание
					о защите ПДн. При пересмотре сроков необходимых изменения должны быть внесены в Положение о защите ПДн
10.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн	При необходимости		Комиссия по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн производится с оформлением Акта на списание и уничтожение электронных (бумажных) носителей информации
11.	Классификация ИСПДн и определение уровня защищенности ИСПДн	При необходимости		Комиссия по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных	Классификация проводится при создании ИСПДн, при выявлении в информационных системах ПДн, при изменении состава, структуры самой ИСПДн или технических особенностей ее построения (изменилось программное обеспечение, топология сети и прочее)
12.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости		Комиссия по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных	Разрабатывается при создании системы защиты ИСПДн
13.	Аттестация (сертификация) СЗПДн или декларирование соответствия по требованиям безопасности ПДн	При необходимости			Проводится совместно с лицензиатами ФСТЭК
14.	Эксплуатация ИСПДн и контроль безопасности ПДн	Постоянно		Ответственный за обеспечение безопасности персональных данных в информационных системах (Главный специалист экспертного отдела культуры и информационного обеспечения)	
15.	Понижение требований по защите ПДн путем сегментирования ИСПДн, отключения от сетей общего	При необходимости		Комиссия по определению уровня защищенности персональных данных при их обработке в информационных	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в

№ п/п	Наименование мероприятия	Срок выполнения	Дата	Ответственный	Примечание
	пользования, обеспечения обмена между ИСПДн с помощью сменных носителей, создания автономных ИСПДн на выделенных АРМ и прочих доступных мер			системах персональных данных	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 Администрации Яльчикского района Чувашской Республики от «26» авг 2016 г.

План внутренних проверок режима защиты персональных данных в Администрации Яльчикского района Чувашской Республики

№	Мероприятие	Периодичность	Исполнитель
1.	Контроль соблюдения режима обработки ПДн	Раз в полгода	Ответственный за организацию обработки персональных данных (Управляющий делами – начальник отдела организационной работы)
2.	Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно	Ответственный за организацию обработки персональных данных (Управляющий делами – начальник отдела организационной работы) Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (Главный специалист эксперт отдела культуры и информационного обеспечения)
3.	Контроль соблюдения режима парольной защиты	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (Главный специалист эксперт отдела культуры и информационного обеспечения)
4.	Контроль выполнения антивирусной защиты	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (Главный специалист эксперт отдела культуры и информационного обеспечения)
5.	Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (Главный специалист эксперт отдела культуры и информационного обеспечения)
6.	Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (Главный специалист эксперт отдела культуры и информационного обеспечения)

7.	Контроль за обеспечением резервного копирования	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (Главный специалист эксперт отдела культуры и информационного обеспечения)
8.	Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	Комиссия по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных
9.	Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	Ответственный за организацию обработки персональных данных (Управляющий делами – начальник отдела организационной работы)
10.	Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями.	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (Главный специалист эксперт отдела культуры и информационного обеспечения)
11.	Тестирование всех функций СЗИ НСД с помощью специальных программных средств	Ежегодно	Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (Главный специалист эксперт отдела культуры и информационного обеспечения)