МУНЩИПАЛЬНИЙ БЮДЖЕТНИЙ ЗАГАЛЬНООСВІТНІЙ ЗАКЛАД «ЗАВІТ-ЛЕНІНСЬКА ШКОЛА – ДИТЯЧИЙ САДОК» ДЖАНКОЙСЬКОГО РАЙОНУ РЕСПУБЛІКИ КРИМ

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ЗАВЕТ-ЛЕНИНСКАЯ ШКОЛА – ДЕТСКИЙ САД ДЖАНКОЙКОГО РАЙОНА РЕСПУБЛИКИ КРЫМ

КЪЫРЫМ ДЖУМХУРИЕТИ ДЖАНКОЙ РАЙОНЫНЫНЪ МУНИЦИПАЛЬ БЮДЖЕТЛИ УМУМТАСИЛЬ МУЭССИСЕСИ «ЗАВЕТ-ЛЕНИНСКИЙ МЕКТЕБИ – БАЛАЛАР БАГЪЧАСЫ»

296126, Российская Федерация, Республика Крым, Джанкойский р-он, с. Завет-Ленинский, ул. Шевченко д.42
e-mail: zavet-leninskaya@yandex.ru

ПРИКАЗ

«16» 02 2022 г. № 62/1

с. Завет-Ленинский

«Об организации работы по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

С целью организации обработки персональных данных в МБОУ «Завет-Ленинская школа – детский сад» в соответствии с пунктом 1 части 1 статьи 18.1 и части 1 статьи 22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Требованиями к защите персональных данных при обработке в информационных системах персональных данных, утвержденными постановлением Правительства от 01.11.2012 № 1119

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие с «16» 02 2022г. в МБОУ «Завет-Ленинская школа – детский сад» Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Приложение 1).
2. Назначить ответственным за организацию работы в АИС «Навигатор дополнительного образования» в МБОУ «Завет-Ленинская школа – детский сад» педагога-организатора Осетрову Анну Витальевну. В своей работе неукоснительно соблюдать правила указанного положения при обработке персональных данных воспитанников и обучающихся в системе АИС.
3. Контроль исполнения приказа оставляю за собой.

Директор Н.А. Забавка

С приказом ознакомлена:
16.02.2022 А.В. Осетрова

Приложение 1
УТВЕРЖДЕНО
приказом МБОУ «Завет-Ленинская
школа – детский сад»
№62/1 от 16.02.2022

Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ «Завет-Ленинская школа – детский сад»

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 МБОУ «Завет-Ленинская школа – детский сад» (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 – ПД) в информационных системах персональных данных (далее – ИСПД) МБОУ «Завет-Ленинская школа – детский сад» (далее – учреждение) на протяжении всего жизненного цикла ИСПД.

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 физическ лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющ обработку персональных данных, а также определяющие цели обработки персональных данны состав персональных данных, подлежащих обработке, действия (операции), совершаемые персональными данными.

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

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

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

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

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

Угрозы безопасности персональных данных – совокупность условий и фактор создающих опасность несанкционированного, в том числе случайного, доступа к персональны данным, результатом которого может стать уничтожение, изменение, блокирование, копирован распространение персональных данных, а также иных несанкционированных действий при обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых становит невозможным восстановить содержание персональных данных в информационной систе персональных данных и (или) в результате которых уничтожаются материальные носите персональных данных.

Уровень защищенности персональных данных – комплексный показате характеризующий требования, исполнение которых обеспечивает нейтрализацию определенн угроз безопасности персональных данных при их обработке в информационных систем персональных данных.

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

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

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

3.1. Под организацией обеспечения безопасности ПД при их обработке в ИСПД понимает формирование и реализация совокупности согласованных по цели, задачам, месту и време организационных и технических мероприятий, направленных на минимизацию ущерба возможной реализации угроз безопасности ПД, реализуемых в рамках создаваемой систе защиты персональных данных (далее – СЗПД).

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

3.3. Безопасность ПД при их обработке в ИСПД обеспечивает учреждение или ли осуществляющее обработку ПД по поручению учреждения на основании заключаемого с эт

лицом договора (далее – уполномоченное лицо). Договор между учреждением и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность ПД при их обработке в информационной системе.

3.4. Выбор средств защиты информации для СЗПД осуществляется учреждением 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 СЗПД определяются исходя из уровня защищенности ПД при их обработке в ИСПД.

3.6. СЗПД создается в три этапа:

Этап 1. Предпроектное обследование ИСПД и разработка технического задания на создание СЗПД.

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

Этап 3. Ввод ИСПД с СЗПД в эксплуатацию.

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

3.7.1. Назначение ответственного за организацию обработки ПД учреждением.

3.7.2. Создание комиссии по определению уровня защищенности ПД при их обработке в ИСПД учреждения.

3.7.3. Определение целей обработки ПД учреждением.

3.7.4. Определение перечня ИСПД учреждения и состава ПД, обрабатываемых в ИСПД.

3.7.5. Определение перечня обрабатываемых учреждением ПД.

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

3.7.7. Определение перечня используемых в ИСПД (предполагаемых к использованию в ИСПД) общесистемных и прикладных программных средств.

3.7.8. Определение режимов обработки ПД в ИСПД в целом и в отдельных компонентах.

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

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

3.7.11. Определение перечня помещений, в которых размещены ИСПД и материальные носители ПД.

3.7.12. Формирование технических паспортов ИСПД.

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

– Политика в отношении обработки персональных данных;

– Инструкции (ответственного за организацию обработки ПД, ответственного за обеспечение безопасности ПД в ИСПД, пользователя ИСПД, ответственного пользователя криптосредств);

– Раздел должностных инструкций сотрудников учреждения в части обеспечения безопасности ПД при их обработке, включая установление персональной ответственности за нарушения правил обработки ПД.

3.7.14. Получение (при необходимости) согласия на обработку ПД субъектом ПД, подписание обязательства о соблюдении конфиденциальности ПД сотрудниками учреждения.

3.7.15. Утверждение форм уведомлений субъектов ПД и форм журналов, необходимых в целях обеспечения безопасности ПД.

3.7.16. Определение уровня защищенности ПД при их обработке в ИСПД в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119

«Об утверждении требований к защите персональных данных при их обработке информационных системах персональных данных» (подготовка и утверждение акта определени уровня защищенности ПД при их обработке в ИСПД).
3.7.17. Определение типа угроз безопасности ПД, актуальных для информационной системы, учетом оценки возможного вреда в соответствии с нормативными правовыми актами, принятым во исполнение Федерального закона «О персональных данных» от 27 июля 2006 г. № 15 Определение угроз безопасности ПД в конкретных условиях функционирования ИСП (разработка моделей угроз безопасности ПД при их обработке в ИСПД).
3.7.18. Формирование технического задания на разработку СЗПД по результатам предпроектно обследования на основе нормативно-методических документов ФСТЭК России и ФСБ России учетом установленного уровня защищенности ПД при их обработке в ИСПД.

Техническое задание на разработку СЗПД должно содержать:

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

3.8. Этап 2. Проектирование СЗПД, закупка, установка, настройка и опытная эксплуатац необходимых средств защиты информации.
3.8.1. Создание СЗПД является необходимым условием обеспечения безопасности ПД, в т случае, если существующие организационные и технические меры обеспечения безопасности соответствуют требованиям к обеспечению безопасности ПД для соответствующего уров защищенности ПД при их обработке в ИСПД и (или) не нейтрализуют всех угроз безопасности П для данной ИСПД.
3.8.2. Технические меры защиты ПД предполагают использование программно-аппаратны средств защиты информации. При обработке ПД с использованием средств автоматизац применение технических мер защиты является обязательным условием, а их количество и степе защиты определяется в процессе предпроектного обследования информационных ресурс учреждения. Применение технических мер должно быть регламентировано локальным акт учреждения.
3.8.3. Средства защиты информации, применяемые в ИСПД, в установленном порядке прохо процедуру оценки соответствия, включая сертификацию на соответствие требованиям безопасности информации.
3.8.4. На стадии проектирования и создания СЗПД для ИСПД учреждения проводятся следующ мероприятия:

– разработка технического проекта СЗПД;
– приобретение (при необходимости), установка и настройка серийно выпускаемых техническ средств обработки, передачи и хранения информации;
– разработка мероприятий по защите информации в соответствии с предъявляемы требованиями;
– приобретение, установка и настройка сертифицированных технических, программных программно-технических средств защиты информации, в том числе (при необходимости) средс криптографической защиты информации;
– реализация разрешительной системы доступа пользователей ИСПД к обрабатываемой в ИСП информации;
– подготовка эксплуатационной документации на используемые средства защиты информации;
– корректировка (дополнение) организационно-распорядительной документации в части защит информации.

3.9. Этап 3. Ввод ИСПД с СЗПД в промышленную эксплуатацию.
3.9.1. На стадии ввода в ИСПД (СЗПД) осуществляются:

– опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПД (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 ПД).

3.9.2. Контроль за выполнением настоящих требований организуется и проводится учреждением (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 учреждением (уполномоченным лицом).

4. ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Работы по обеспечению безопасности ПД проводятся в соответствии с Планом мероприятий по защите персональных данных (ПРИЛОЖЕНИЕ № 1). Внутренние проверки режима обработки и защиты ПД учреждением 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 учреждении (ПРИЛОЖЕНИЕ № 3).

4.2. Контроль за проведением работ по обеспечению безопасности ПД осуществляет ответственный за организацию обработки ПД в виде методического руководства, участия в разработке требований по защите ПД, организации работ по выявлению возможных каналов утечки информации, согласования выбора средств вычислительной техники и связи, технических и программных средств защиты, участия в оценке соответствия ИСПД учреждения требованиям безопасности ПД.

4.3. При необходимости к проведению работ по обеспечению безопасности ПД 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 с 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 СЗПД средств криптографической защиты информации к проведению работ по обеспечению безопасности ПД учреждению 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 УЧРЕЖДЕНИЯ

5.1. Настоящий порядок определяет правила проведения резервного копирования данны обрабатываемых в ИСПД учреждения.

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

5.3. Резервному копированию подлежит информация, обрабатываемая в ИСПД учреждения.

5.4. В учреждении должна быть реализована централизованная система резервного копирования.

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

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

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

– работоспособности средств резервного копирования и восстановления;

– готовности информационных ресурсов к осуществлению их резервного копирования и восстановления;

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

5.7. Расписание проведения резервного копирования определяется Ответственным.

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

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

5.10. В случае выявления нарушений Ответственному необходимо в кратчайшие сроки устрани неисправности в системе резервного копирования и восстановить работоспособность подсистем штатный режим работы.

5.11. О выявленных попытках несанкционированного доступа к резервируемой информации, также иных нарушениях информационной безопасности, произошедших в процессе резервно копирования, Ответственный сообщает руководству учреждения немедленно.

5.12. Ответственный должен контролировать проведение резервного копирования в цел выполнения требований по защите информации.

5.13. В случае обнаружения ошибки резервного копирования Ответственный выполняет повторн копирование информации вручную в максимально сжатые сроки, не нарушая технологическ процессы обработки информации пользователями учреждения, в Журнал резервного копирован и восстановления информации заносятся соответствующие отметки.

5.14. Хранение резервных копий данных осуществляется на сменных носителях информац (CD/DVD, внешние жесткие диски и т.п.), промаркированных Ответственным в соответствии расписанием резервного копирования. Маркировка должна содержать номер копии, дату создания, наименование ИСПД.

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

5.16. Срок хранения резервных копий определяется Ответственным.

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

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

5.19. Основанием для инициирования процедуры восстановления служит полная или частичн утрата информации вследствие сбоев оборудования, программного обеспечения, в критических 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 СЗПД для функционирующих ИСПД учреждения должна осуществляться в случае:
– изменения состава или структуры ИСПД или технических особенностей ее построения (изменения состава или структуры программного обеспечения, технических средств обработки ПД, топологии ИСПД);
– изменения состава угроз безопасности ПД в ИСПД;
– изменения уровня защищенности ПД при их обработке в ИСПД;
– прочих случаях, по решению учреждения.
6.2. В целях определения необходимости доработки (модернизации) СЗПД не реже одного раза в год ответственным за организацию обработки ПД должна проводиться проверка состава и структуры ИСПД, состава угроз безопасности ПД в ИСПД и уровня защищенности ПД при их обработке в ИСПД, соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Результаты проверки оформляются актом проверки и утверждаются руководителем учреждения.
6.3. Анализ инцидентов безопасности ПД и составление заключений в обязательном порядке должно проводиться в случае выявления следующих фактов:
– несоблюдение условий хранения носителей ПД;
– использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) ПД или другим нарушениям, приводящим к снижению уровня защищенности ПД;
– нарушение заданного уровня безопасности ПД (конфиденциальность/ целостность/доступность).

Приложение № 1

План мероприятий по защите персональных данных
в МБОУ «Завет-Ленинская школа – детский сад»

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
1.	Документальное регламентирование работы с ПД	При необходимости	Разработка организационно-распорядительных документов по защите ПД, либо внесение изменений в существующие
2.	Получение согласий субъектов ПД (физических лиц) на обработку ПД в случаях, когда этого требует законодательство	Постоянно	В случаях, предусмотренных Федеральным законом «О персональных данных», обработка ПД осуществляется только с согласия в письменной форме субъекта ПД. Форма согласия приведена в Приказе «Об утверждении форм документов, необходимых в целях выполнения требований законодательства в области персональных данных». Равнозначным содержащему собственноручную подпись субъекта ПД 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 ПД	При необходимости	В случае поручения обработки ПД субъектов ПД третьим лицам (например, кредитно-финансовым учреждениям) в договор включается пункт о соблюдении конфиденциальности при обработке ПД, а также учитываются требования ч.3 ст.6 Федерального закона «О персональных данных»
4.	Ограничение доступа сотрудников к ПД	При необходимости (при создании ИСПД)	В случае создания ИСПД, а также приведения имеющихся ИСПД в соответствие с требованиями закона необходимо разграничить доступ сотрудников учреждения к ПД
5.	Взаимодействие с субъектами ПД	Постоянно	Работа с обращениями субъектов ПД, ведение журналов учета передачи персональных данных, обращений субъектов ПД, уведомление субъектов ПД об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПД, получении ПД от третьих лиц.
6.	Ведение журналов учета электронных носителей персональных данных, средств защиты информации	Постоянно	
7.	Повышение квалификации сотрудников в области защиты ПД	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 ПД в ИСПД).
8.	Инвентаризация информационных ресурсов	Раз в полгода	Проводится с целью выявления в информационных ресурсах присутствия ПД.
9.	Установка сроков обработки ПД и процедуры их	При необходимости	Для уничтожения ПД учреждением устанавливаются сроки обработки ПД, которые документально подтверждаются в локальных

	уничтожения по окончании срока обработки		актах учреждения. При пересмотре сроков необходимые изменения вносятся в соответствующие документы
10.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПД	При необходимости	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПД 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 ПД при их обработке в ИСПД	При необходимости	Определение уровня защищенности ПД при их обработке в ИСПД осуществляется при создании ИСПД, при изменении состава ПД, объема обрабатываемых ПД, субъектов ПД.
12.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости	Разрабатывается при создании системы защиты ИСПД.
13.	Аттестация ИСПД на соответствие требова-ниям по обеспечению безопасности ПД	При необходимости	Проводится совместно с лицензиатами ФСТЭК
	Эксплуатация ИСПД и контроль безопасности ПД	Постоянно	
	Понижение требований по защите ПД путем сегментирования ИСПД, отключения от сетей общего пользования, обеспечения обмена между ИСПД с помощью сменных носителей, создания автономных ИСПД на выделенных АРМ и прочих доступных мер	При необходимости	В случае создания ИСПД, а также приведения имеющихся ИСПД в соответствии с требованиями закона

Приложение № 2

План внутренних проверок режима обработки и защиты персональных данных в МБОУ «Завет-Ленинская школа – детский сад»

№ п/п	Мероприятие	Периодичность	Дата, подпись исполнителя
1.	Осуществление внутреннего контроля и (или) аудита соответствия обработки ПД ФЗ-152 «О персональных данных» и принятым в соответствии с ним нормативным правовым актам	Раз в полгода	
2.	Проверка ознакомления сотрудников, непосредственно осуществляющих обработку ПД, с положениями законодательства Российской Федерации о ПД, в том числе требованиями к защите ПД.	Раз в полгода	
3.	Проверка получения согласий субъектов ПД на обработку ПД в случаях, когда этого требует законодательство	Раз в полгода	
4.	Проверка подписания сотрудниками, осуществляющими обработку ПД, основных форм, необходимых в целях выполнения требований законодательства в сфере обработки и защиты ПД: - Уведомления о факте обработки ПД без использования средств автоматизации; - Обязательства о соблюдении конфиденциальности ПД; - Формы ознакомления с положениями законодательства Российской Федерации о ПД, локальными актами учреждения по вопросам обработки ПД; - Разъяснения субъекту ПД юридических последствий отказа предоставить свои ПД.	Раз в полгода	
5.	Проверка уничтожения материальных носителей ПД с составлением соответствующего акта	Ежегодно	
6.	Проверка ведения журналов по учету обращений субъектов ПД и учету передачи ПД субъектов третьим лицам	Раз в полгода	
7.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПД	Ежегодно	
8.	Проверка соблюдения условий хранения материальных носителей ПД	Раз в полгода	
9.	Проверка состояния актуальности Уведомления об обработке (намерении осуществлять обработку) ПД.	Раз в полгода	
10.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПД, в том числе документов, определяющих политику учреждения в отношении обработки ПД.	Раз в полгода	
11.	Организация анализа и пересмотра имеющихся угроз безопасности ПД, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	
12.	Оценка вреда, который может быть причинен субъектам ПД в случае нарушения ФЗ-152 «О персональных данных»	Ежегодно	
13.	Проверка применения для обеспечения безопасности ПД средств защиты информации, прошедших в установленном порядке процедуру соответствия	Раз в полгода	
14.	Оценка эффективности принимаемых мер по обеспечению безопасности ПД до ввода в эксплуатацию ИСПД	При необходимости	
15	Контроль учета машинных носителей ПД	Раз в полгода	
16	Контроль за принимаемыми мерами по обеспечению безопасности ПД и уровня защищенности ПД в ИСПД	Раз в полгода	
17	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий	Ежеквартально	

	пользователей в ИСПД		
18	Контроль внесения изменений в структурно-функциональные характеристики ИСПД	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 ПД	Раз в полгода	

Приложение № 3

Отчет о результатах проведения внутренней проверки режима обработки и защиты персональных данных
в МБОУ «Завет-Ленинская школа – детский сад»

1.1 Внутренняя проверка произведена на основании Положения по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ «Завет-Ленинская школа – детский сад» 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 ПД рекомендуется осуществить следующие мероприятия:
1) _____
2) _____
3) _____
4) _____
5) _____

Подписи ответственных лиц, проводивших внутреннюю проверку режима обработки и защиты ПД:

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

Приложение № 4

Журнал резервного копирования/восстановления данных

Схема резервного копирования/восстановления данных	Копируемые/восстанавливаемые ресурсы	Хранилище	Дата/время создания копии/восстановления	Фамилия ответственного	Подпись ответственного	Результат резервного копирования/восстановления данных	Комментарий
2	3	4	5	6	7	8	9