Приложение № 1
к Приказу № 117 от 03.09.2018г.

**Политика МБДОУ ДС №48 «Одуванчик» г. Светлоград
в области обработки персональных данных**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В целях поддержания деловой репутации и гарантирования выполнения форм федерального законодательства в полном объеме муниципальное бюджетное дошкольное образовательное учреждение детский сад №48 «Одуванчик» г. Светлоград (далее МБДОУ ДС №48 «Одуванчик» г. Светлоград, Оператор) считает важнейшими своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечение безопасности процессов их обработки.

1.2. Настоящая политика в области обработки и защиты персональных данных в МБДОУ ДС №48 «Одуванчик» г. Светлоград (далее – Политика) характеризуется следующими признаками:

1.2.1. Разработана в целях обеспечения реализации требований законодательства РФ в области обработки персональных данных субъектов персональных данных.

1.2.2. Раскрывает основные категории персональных данных, обрабатываемых Оператором, цели, способы и принципы обработки Оператором персональных данных, права и обязанности Оператора при обработке персональных данных, права субъектов персональных данных, а также включает перечень мер, применяемых Оператором в целях обеспечения безопасности персональных данных при их обработке.

1.2.3. Является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке персональных данных.

2. ИНФОРМАЦИЯ ОБ ОПЕРАТОРЕ

Наименование: муниципальное бюджетное дошкольное образовательное учреждение детский сад №48 «Одуванчик» г. Светлоград

Фактический адрес: 356530, Ставропольский край, Петровский городского округа, г. Светлоград, улица Урожайная, 2и.

Тел.: 8(865-47) 4-51-21.

3. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Политика Оператора в области обработки персональных данных определяется в соответствии со следующими нормативными правовыми актами РФ:

3.1.1. Конституцией Российской Федерации.

3.1.2. Трудовым кодексом Российской Федерации.

3.1.3. Гражданским кодексом Российской Федерации.
3.1.4. Федеральным законом от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» (в действующей редакции).
3.1.5. Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (в действующей редакции).
3.1.6. Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в действующей редакции).
3.2. Во исполнение настоящей Политики руководящим органом Оператора утверждены следующие локальные нормативные правовые акты:
3.2.1. Положение об ответственном за организацию обработки персональных данных МБДОУ ДС №48 «Одуванчик» г. Светлоград;
3.2.2. Положение о защите персональных данных МБДОУ ДС №48 «Одуванчик» г. Светлоград;
3.2.3.Положение об организации работы с персональными данными работников МБДОУ ДС №48 «Одуванчик» г.Светлоград;
3.2.4.Положение об организации работы с персональными данными воспитанников МБДОУ ДС №48 «Одуванчик» г.Светлоград;
3.2.5.Перечень подразделений и должностей, осуществляющих обработку персональных данных в МБДОУ ДС №48 «Одуванчик» г.Светлоград.

4. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Оператор обрабатывает персональные данные исключительно в следующих целях:
4.1.1. Исполнения положений нормативных актов, указанных в п. 2.2.1.
4.1.2. Принятия решения о трудоустройстве работников в МБДОУ ДС №48 «Одуванчик» г. Светлоград.
4.1.3. Оказания услуг в области образования.
4.1.4. Сбора и анализа информации, создания базы данных в МБДОУ ДС №48 «Одуванчик» г. Светлоград.
4.1.5. Повышения квалификации педагогических работников и административно - управленческого персонала, других сотрудников МБДОУ ДС №48 «Одуванчик» г. Светлоград.
4.1.6. Обеспечение условий выполнения трудовых обязанностей сотрудников МБДОУ ДС №48 «Одуванчик» г. Светлоград.

5. КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, ИСТОЧНИКИ ИХ ПОЛУЧЕНИЯ, СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ

5.1. В информационных системах персональных данных Оператора обрабатываются следующие категории персональных данных:
5.1.1. Персональные данные лиц, имеющих трудовые отношения с МБДОУ ДС №48 «Одуванчик» г. Светлоград, сотрудников, а также их родственников,

кандидатов для приема на работу. Источники получения: субъекты персональных данных МБДОУ ДС №48 «Одуванчик» г. Светлоград.
5.1.2. Персональные данные воспитанников МБДОУ ДС №48 «Одуванчик» г. Светлоград их родителей (законных представителей). Источник получения: субъекты персональных данных.
5.1.3. Персональные данные посетителей. Источники получения: субъекты персональных данных МБДОУ ДС №48 «Одуванчик» г. Светлоград.
5.2. Сроки обработки и хранения персональных данных определены в «Перечень подразделений и должностей, осуществляющих обработку персональных данных в МБДОУ ДС №48 «Одуванчик» г. Светлоград (см. п. 3.2.5).

6. ОСНОВНЫЕ ПРИНЦИПЫ ОБРАБОТКИ, ПЕРЕДАЧИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Оператор в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст. 5 Федерального закона 152-ФЗ «О персональных данных».
6.2. Оператор не осуществляет обработку биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).
6.3. Оператор не выполняет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.
6.4. Оператор не производит трансграничную (на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.
6.5. Оператором созданы общедоступные источники персональных данных (справочники, адресные книги). Персональные данные, сообщаемые субъектом (фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и др.), включаются в такие источники только с письменного согласия субъекта персональных данных.

7. СВЕДЕНИЯ О ТРЕТЬИХ ЛИЦАХ, УЧАСТВУЮЩИХ В ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Оператор в ходе своей деятельности предоставляет персональные данные следующим организациям:
7.1.1. Федеральной налоговой службе.
7.1.2. Пенсионному фонду России.
7.1.3. Негосударственным пенсионным фондам.
7.1.4. Образовательным организациям и организациям образования.

7.1.5. Страховым компаниям.
7.1.6. Кредитным организациям.
7.1.7. Лицензирующим и/или контролирующим органам государственной власти и местного самоуправления.
7.2. Оператор не поручает обработку персональных данных другим лицам на основании договора.

8. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

8.1. Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:
8.1.1. Назначением ответственных за организацию обработки персональных данных, мест хранения персональных данных.
8.1.2. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения трудовых обязанностей, допускаются к соответствующим персональным данным на основании утвержденного списка.
8.1.3. В отношении данных, содержащихся в информационных системах – ограничение доступа к электронным носителям, использование парольной защиты. В отношении данных, содержащихся на бумажных носителях – использование сейфов, металлических шкафов, ограничение доступа в помещение.
8.2. Обязанности должностных лиц, осуществляющих обработку и защиту персональных данных, а также их ответственность, определяются в «Положение о защите персональных данных МБДОУ ДС №48 «Одуванчик» г.Светлоград (см. п. 3.2.2).

9. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ.

9.1. Субъект персональных данных имеет право на получение сведений об обработке его персональных данных Оператором.
9.2. Субъект персональных данных вправе требовать от Оператора, который их обрабатывает, уточнения этих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.

11.1. Настоящая Политика разрабатывается и утверждается приказом заведующего МБДОУ ДС №48 «Одуванчик» г. Светлоград.

11.2. Настоящая Политика обязательна для соблюдения и подлежит доведению до всех сотрудников МБДОУ ДС №48 «Одуванчик» г. Светлоград.
11.3. Контроль за соблюдением Политики осуществляет заведующий МБДОУ ДС №48 «Одуванчик» г. Светлоград.

Приложение № 2
к Приказу № 117 от 03.09.2018г.

ПОРЯДОК
уничтожения, блокирования персональных данных в МБДОУ ДС №48 «Одуванчик» г. Светлоград

1. Общие положения

1.1.Настоящий Порядок уничтожения, блокирования персональных данных в МБДОУ ДС №48 «Одуванчик» г. Светлоград определяет условия и способы:

- уничтожения бумажных носителей (документов), содержащих персональные данные по достижению цели обработки этих персональных данных;
- персональных данных в машинных носителях информации, в том числе персональных данных, и при необходимости самих машинных носителей информации.

2. Блокирование и уничтожение персональных данных, содержащихся в машинных носителях информации.

2.1. Блокирование информации, содержащей персональные данные субъекта персональных данных, производится в случаях:

- если персональные данные являются неполными, устаревшими, недостоверными;
- если сведения являются незаконно полученными или не являются необходимыми для заявленной оператором персональных данных цели обработки.

2.2. В случае подтверждения факта недостоверности персональных данных уполномоченное Оператором лицо на основании документов, представленных субъектом персональных данных, уполномоченным органом по защите прав субъектов персональных данных или полученных в ходе самостоятельной проверки, обязано уточнить персональные данные и снять их блокирование.

2.3. В случае выявления неправомерных действий с персональными данными уполномоченное Оператором лицо обязано устранить (организовать устранение) допущенные нарушения. В случае невозможности устранения допущенных нарушений необходимо в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожить персональные данные.

2.4. Об устранении допущенных нарушений или об уничтожении персональных данных уполномоченное Оператором лицо обязано уведомить субъекта персональных данных, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

2.5. Уполномоченное Оператором: лицо обязано уничтожить персональные данные субъекта персональных данных в случаях:

- достижения цели обработки персональных данных оператор;

- отзыва субъектом согласия на обработку своих персональных данных.

2.6. Уничтожение персональных данных должно быть осуществлено в течение трех дней с указанных моментов. В согласии субъекта персональных данных на обработку его персональных данных могут быть установлены иные сроки уничтожения персональных данных при достижении цели обработки персональных данных.

3. Работа с бумажными носителями (документами)

3.1. Виды и периоды уничтожения бумажных носителей, содержащих персональные данные, представлены в таблице 1:

Таблица 1

п/п	Документ	Срок хранения	Действия по окончанию срока хранения
1.	Документы (сведения, содержащие персональные данные о работниках Оператора), переданные и сформированные при трудоустройстве работника.	75 лет	Уничтожение
2.	Документы о воспитанниках (сведения, содержащие персональные данные воспитанников), родителей (законных представителей)	установленные для данных документов сроки хранения	Уничтожение
3.	Другие документы с грифом «Конфиденциально» и «Для служебного пользования» (Журналы учёта, списки доступа, эксплуатационная документация и т.п.)	хранятся до замены на новые, если не указан конкретный срок	Уничтожение

3.2 Документы, указанные в п. 3.1, должны находиться в шкафах с замком, сейфах с доступом к ним сотрудника отдела кадров или уполномоченных лиц. Исключение составляют документы, обрабатываемые в настоящий момент на рабочем месте.

3.3. По окончании срока хранения документы, указанные в п. 3.1., уничтожаются путём измельчения на мелкие части (или иным способом), исключающие возможность последующего восстановления информации или сжигаются.

4. Работа с машинными носителями информации

4.1. Виды и периоды уничтожения персональных данных, хранимых в электронном виде («файлах») на жестком диске компьютера (далее - НЖМД) и машинных носителях: компакт дисках (далее - CD-R/W, DVD-R/RW в зависимости от формата), FLAS-накопителях.

Таблица 2

№ п/п	Информация, вид носителя	Срок хранения	Действия по окончании срока хранения
1.	База данных автоматизированной информацией системы Оператора Носитель; файлы на НЖМД сервера	До создания более актуальной копии	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности - уничтожение носителя; удаление архивных файлов с НЖМД
2.	База данных автоматизированной информационной системы «Аверс». Носитель: файлы на НЖМД сервера	До создания более актуальной копии	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности - уничтожение носителя; удаление архивных файлов с НЖМД

4.2 Машинные носители информации (за исключением НЖМД), перечисленные в п.п. 3.1. должны находиться в сейфе, кроме формируемых или обрабатываемых в данный момент на рабочем месте.
4.3 По окончании указанных сроков хранения, машинные носители информации, подлежащие уничтожению, физически уничтожаются с целью невозможности восстановления и дальнейшего использования. Это достигается путём: деформирования, нарушения единой целостности носителя или его сжигания.
4.4. Подлежащие уничтожению файлы, расположенные на жестком: диске компьютера, удаляются средствами операционной системы с последующим «очищение корзины».
4.5 . В случае допустимости повторного использования носителя формата CD- RW, DRW, FLASH применяется программное удаление («затирание») содержимого диска путём его форматирования с последующей записью новой информации на данный носитель,
5. Порядок оформления документов об уничтожении носителей
5.1 Уничтожение носителей, содержащих персональные данные, осуществляет специальная Комиссия, создаваемая приказом руководителя Оператора.
5.2 В ходе процедуры уничтожения персональных данных носителей необходимо присутствие членов Комиссии, осуществляющей уничтожение персональных данных и иной конфиденциальной информации, находящейся на технических средствах.
5.3 Комиссия составляет и подписывает Акт об уничтожении носителей. В течение трёх дней после составления акты об уничтожении направляются на

утверждение руководителю Оператора. После утверждения Акт хранится в сейфе у руководителя соответствующего подразделения Оператора

5.4 Факт уничтожения носителя с персональными данными фиксируется в «Журнале регистрации носителей информации, содержащих персональные данные и иную конфиденциальную информацию», где в графе «Дата и номер акта уничтожения» заносятся соответствующие данные. Данный журнал является документом конфиденциального характера и вместе с актами уничтожения хранится в сейфе.

Приложение № 3
к Приказу № 117 от 03.09.2018г.

ЖУРНАЛ УЧЕТА ВНУТРЕННЕГО ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКОВ

Дата выдачи документа (личного дела)	Дата возврата документа (личного дела)	Наименования документа (личного дела)	Цель выдачи	ФИО, подпись получившего документ (личное дело) на временное пользование	ФИО, подпись лица, принявшего документ(личное дело) на хранение
1.	2.	3.	4.	5.	6.

Приложение № 4
к Приказу № 117 от 03.09.2018г.

ЖУРНАЛ УЧЕТА ВЫДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ ДОУ

№	Сведения о запрашивающем лице	Состав и принадлежность запрашиваемых персональных данных	Цель получения персональных данных	Дата запроса персональных данных	Дата передачи/ отказа в передаче персональных данных	Дата возврата документов	Подпись запрашивающего лица	Подпись ответственного сотрудника

Приложение № 5
к Приказу № 117 от 03.09.2018г.

ЖУРНАЛ ПРОВЕРОК НАЛИЧИЯ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ РАБОТНИКОВ

Дата проверки	ФИО проверяющего	Цель проверки	Замечания
1.	2.	3.	4.

Приложение № 6
к Приказу № 117 от 03.09.2018г.

АКТ № _____
об уничтожении персональных данных
субъекта(ов) персональных данных, обрабатываемых
в _____

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

составила настоящий Акт о том, что информация, зафиксированная на перечисленных в нем носителях информации (электронных, бумажных), подлежат уничтожению.

Учетный номер материального носителя, номер дела и т.д.	Причина уничтожения носителя информации; стирания/обезличивания информации	Тип носителя информации	Производимая операция (стирание, уничтожение, обезличивание)	Дата
1.	2.	3.	4.	5.

Приложение № 7
к Приказу № 117 от 03.09.2018г.

Инструкция по организации парольной защиты

1. Общие положения

Настоящая инструкция устанавливает основные правила введения парольной защиты информационной системы персональных данных МБДОУ ДС № 48 «Одуванчик» г. Светлоград(далее – Учреждение). Инструкция регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в информационной системы персональных данных, а также контроль за действиями пользователей системы при работе с паролями.

Настоящая инструкция оперирует следующими основными понятиями:

− Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

− ИСПДн – информационная система персональных данных.

− Компрометация- факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

− Объект доступа - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

− Пароль – уникальный признак субъекта доступа, который является его (субъекта) секретом.

− Правила доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

− Субъект доступа - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

− Несанкционированный доступ - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АС.

2. Правила генерации паролей

2.1 Персональные пароли должны генерироваться специальными программными средствами административной службы.

2.2 Длина пароля должна быть не менее 8 символов.

2.3 В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.

2.4 Пароль не должен включать в себя: − легко вычисляемые сочетания символов; − клавиатурные последовательности символов и знаков; − общепринятые сокращения; − аббревиатуры; − номера телефонов, автомобилей; − прочие сочетания букв и знаков, ассоциируемые с пользователем; − при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 2 символа.

2.5 Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПДн объекта образования.

3. Порядок смены паролей

3.1 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одно раза в месяц.
3.2 Полная внеплановая смена паролей всех пользователей должна производиться случае прекращения полномочий администраторов средств защиты или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной зашитой.
3.3 Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИСПДн.
3.4 В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

4. Обязанности пользователей при работе с парольной защитой

4.1 При работе с парольной защитой пользователям запрещается:
− разглашать кому-либо персональный пароль и прочие идентифицирующие сведения;
− предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПДн посторонним лицам;
− записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.
4.2 Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.
4.3 При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

5. Случаи компрометации паролей

5.1 Под компрометацией следует понимать:
− физическая утеря носителя с информацией;
− передача идентификационной информации по открытым каналам связи;
− проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);
− визуальный осмотр носителя идентификационной информации посторонним лицом;
− перехват пароля при распределении идентификаторов;
− сознательная передача информации постороннему лицу.
5.2 Действия при компрометации пароля:
− скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль;
− о компрометации немедленно оповещаются все участники обмена информацией. Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

6. Ответственность пользователей при работе с парольной защитой

6.1 Повседневный контроль за действиями сотрудников Учреждения при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается

на ответственного за систему защиты информации в информационной системе персональных данных.
6.2 Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.
6.3 Ответственность за организацию парольной защиты возлагается на ответственного за систему защиты информации в информационной системе персональных данных.
6.4 Ответственность в случае несвоевременного уведомлении ответственного за систему защиты информации в информационной системе персональных данных о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.

Приложение № 8
к Приказу № 117 от 03.09.2018г.

Положение
Муниципального бюджетного дошкольного образовательного учреждения детского сада №48 «Одуванчик» г. Светлоград об обработке и обеспечении безопасности персональных данных

1. Термины и определения

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники; Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Доступ к персональным данным - возможность получения персональных данных и их пользования.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных - обязательное для выполнения оператором и иными лицами, получившими доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

Предоставление персональных данных - действия, направленные на получение персональных данных определенным кругом лиц или передачу персональных данных определенному кругу лиц.

Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими не него право.

2. Назначение и область применения

Настоящее Положение об обработке и обеспечении безопасности персональных данных (далее - Положение) муниципального бюджетного дошкольного образовательного учреждения детского сада №48 «Одуванчик» г. Светлоград (далее Организация).

Разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 152 - ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 01.11.2012 № 1119 « Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и от 15.09. 2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Трудовым кодексом Российской Федерации, иными нормативными правовыми актами, действующими на территории Российской Федерации.

Положение определяет порядок обработки и обеспечения безопасности персональных данных (далее - ПДн) в Организации, устанавливает процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, определяет права, обязанности и ответственность лиц, допущенных к обработке ПДн и ответственных за организацию обработки ПДн.

Действие настоящего Положения распространяется на все процессы обработки персональных данных в Организации, как с использованием средств автоматизации, так и без использования таких средств, на все структурные подразделения и работников Организации, участвующих в таких процессах, а также на информационные системы Организации, используемые в процессах обработки ПДн. Настоящее Положение вступает в силу с момента его утверждения директором Организации и действует бессрочно, до замены его новым Положением. Все изменения в Положение вносятся приказом. Положение обязательно для соблюдения всеми работниками Организации и должно быть доведено до них под подпись. Контроль за соблюдением настоящего Положения, осуществляется лицом, ответственным за организацию обработки персональных данных в Организации, которое назначается приказом директора Организации.

3. Принципы обработки персональных данных.

Обработка персональных данных осуществляется Организацией на законной и справедливой основе и ограничивается достижением конкретных, заранее определенных и законных целей.

Организацией не допускается обработка персональных данных, несовместимая с целями сбора персональных данных и объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых Организацией персональных данных соответствуют заявленным целям обработки, избыточность обрабатываемых данных не допускается.

При обработке персональных данных Организацией обеспечивается точность персональных данных, их достаточность и в необходимых случаях актуальность по отношению к целям обработки персональных Организацией принимаются необходимые меры (обеспечивается их принятие) по удалению или уточнению неполных или неточных персональных данных.

Хранение персональных данных Организацией осуществляется в форме позволяющей определить субъекта персональных данных, не дольше чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

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

При определении состава обрабатываемых персональных данных субъектов персональных данных Организация руководствуется минимально необходимым составом персональных данных для достижения целей получения персональных данных.

4. Условия обработки персональных данных.

Обработка персональных данных осуществляется в соответствии с целями, заранее определенными и заявленными при сборе персональных данных, а также полномочиями Организации, определенными действующим законодательством Российской Федерации и договорными отношениями с Организацией.

Получение и обработка персональных данных в случаях, предусмотренных Федеральным законом от 27.07.2006 152-ФЗ «О персональных данных», осуществляется Организацией с письменного согласия субъекта персональных данных.

Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью.

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не

установлено Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Организацией.

Организация вправе обрабатывать персональные данные без согласия субъекта персональных данных (или при отзыве субъектом персональных данных согласия на обработку персональных данных) при наличии оснований, указанных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных».

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, Организацией не осуществляется.

Сведения, которые характеризуют физиологические особенности! человека и на основе которых можно установить его личность (биометрические персональные данные) и сведения о состоянии здоровья, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных или иных оснований, предусмотренных федеральным законодательством.

Персональные данные субъекта могут быть получены организацией от лица, не являющегося субъектом персональных данных, при условии предоставления организации подтверждения наличия оснований, указанных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных» или иных оснований предусмотренных федеральным законодательством.

Право доступа к персональным данным субъектов персональных данных на бумажных и электронных носителях имеют работники Организации в соответствии с их должностными обязанностями. Право доступа к персональным данным субъектов персональных данных на бумажных и электронных носителях имеют работники Организации в соответствии с их должностными обязанностями.

Организацией не осуществляется трансграничная передача персональных данных и не принимаются решения, основанные исключительно на автоматизированной обработке персональных данных субъекта.

5. Цели обработки персональных данных.

В соответствии с принципами и условиями обработки персональных данных, Организацией определены цели обработки персональных данных:

- организация учебного процесса и контроль качества образования;
- учет и анализ успеваемости учащихся, организация информирования родителей (законных представителей) об успеваемости детей;
- выполнение обязательств, предусмотренных Трудовым договором;

- выполнение требований Трудового кодекса РФ и других нормативных актов РФ (в том числе предоставление персональных данных в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования);

- принятие решений и выполнение обязательств по обращениям граждан Российской Федерации в соответствии с законодательством РФ;

- оказание государственных услуг гражданам.

6. Особенности обработки персональных данных.

Обработка персональных данных Организацией осуществляется как с использованием средств автоматизации, так и без использования таких средств.

При обработке персональных данных Организация осуществляет следующие действия с персональными данными: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

7. Порядок обработки персональных данных.

7.1. Источники получения персональных данных Организация получает ПДн из следующих источников:

- непосредственно от субъекта ПДн;
- от третьей стороны, в целях исполнения договорных обязательств или исполнения требовании нормативных документов РФ.

Если предоставление ПДн является обязательным в соответствии с федеральным законом и субъект ПДн отказывается их предоставить, необходимо разъяснить субъекту ПДн юридические последствия такого отказа.

Если ПДн получены не от субъекта ПДн, то до начала обработки таких ПДн необходимо предоставить субъекту ПДн следующую информацию:

- Цель обработки ПДн и ее правовое основание;
- Предполагаемые пользователи ПДн;
- Установленные законодательством права субъекта ПДн;
- Источник получения ПДн.

Указанная информация может не предоставляться в следующих случаях:

- субъект ПДн уже уведомлен об осуществлении обработки его ПДн соответствующим оператором;
- ПДн получены на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;

- предоставление субъекту ПДн указанных сведений нарушает права и законные интересы третьих лиц.

7.2. Перечень процессов и категорий персональных данных обрабатываемых в Организации Перечень процессов обработки персональных данных, категории субъектов ПДн, чьи данные обрабатывается в Организации, и состав таких данных закреплены в Перечне процессов и персональных данных, обрабатываемых в Организации.

7.3. Способы обработки персональных данных Обработка персональных данных в Организации осуществляется как автоматизированным способом, так и без использования средств автоматизации (на бумажных носителях) работниками Организации, доступ которых к персональным данным, необходим для выполнения ими служебных (трудовых) обязанностей. Документы, содержащие персональные данные, создаются путём:

- копирования оригиналов (паспорт, доверенность, свидетельство ИНН, пенсионное свидетельство и т.д.)
- внесения сведений в учётные формы на бумажных и электронных носителях;
- внесения сведений в информационные системы персональных данных;
- получения оригиналов необходимых документов (трудовая книжка, анкета, и т.д.).

Работники Организации, допущенные к обработке персональных данных в информационных системах персональных данных несут ответственность за достоверность и полноту введенной информации.

7.4. Порядок обработки отдельных документов (типовых форм), содержащих персональные данные.

При использовании внутренних типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее -типовая форма), должны выполняться следующие условия:

в типовые формы или связанные с ними документы (инструкции по заполнению карточки, реестры и журналы) включаются следующие сведения:

-цели обработки ПДн;

-наименование и адрес Организации;

-Ф.И.О. адрес места жительства субъекта ПДн;

- источник получения ПДн (третьи стороны, субъект ПДн и т.п.);

-сроки обработки ПДн; перечень действий, которые будут совершаться с ПДн в процессе их обработки.

- в случае необходимости получения согласия на обработку ПДн (например, отсутствует договор, в рамках исполнения которого необходима обработка ПДн), во внутреннюю типовую форму включается поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн;

- внутренняя типовая форма составляется таким образом, чтобы каждый из субъектов, чьи ПДн содержатся в типовой форме, имел возможность ознакомиться со своими ПДн, не нарушая прав и законных интересов иных субъектов ПДн;

- во внутренней типовой форме не допускается объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо несовместимы.

7.5. Хранение, блокирование и уничтожение персональных данных Персональные данные, позволяющие определить субъекта, хранятся не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по достижении целей обработки персональных данных, или утраты необходимости в их достижении. Законодательством РФ могут устанавливаться специальные сроки хранения отдельных видов документов, содержащих ПДн. В этом случае указанные документы подлежат уничтожению по истечению установленных сроков хранения. Документы, содержащие ПДн, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации. Конкретные обязанности по хранению документов возлагаются на лиц, осуществляющих обработку ПДн, в соответствии с их трудовыми функциями и закрепляются в трудовых договорах, должностных инструкциях и иных регламентирующих документах Организации. Порядок учета материальных носителей ПДн определен в разделе настоящего Положения. Организация блокирует обрабатываемые ПДн при выявлении недостоверности обрабатываемых ПДн или неправомерных действий в отношении субъекта в следующих случаях:

- по требованию субъекта ПДн;
- по требованию уполномоченного органа по защите прав субъектов ПДн (Роскомнадзора),
- по результатам внутренних контрольных мероприятий.

Организация уничтожает персональные данные в следующих случаях:

- по достижению цели обработки персональных данных (в том числе истечении установленных сроков хранения);
- отзыва субъектом согласия на обработку своих персональных когда это согласие является обязательным условием обработки ПДн;
- невозможности устранения допущенных при их обработке нарушений;
- получения соответствующего предписания от уполномоченного органа по защите прав субъектов ПДн.

8. Доступ к персональным данным.

8.1. Предоставление прав доступа к персональным данным.

Персональные данные, обрабатываемые в Организации, относятся к информации ограниченного доступа. Доступ к персональным данным должен быть ограничен, в том числе путем определения перечня лиц, доступ которых к персональным данным, необходим для выполнения ими служебных (трудовых) обязанностей.

При получении доступа к ПДн работники Организации подписывают Соглашение о неразглашении персональных данных. Отсутствие подписанного Соглашения не является основанием для допустимости

нарушения работником конфиденциальности персональных данных, снятия или уменьшения его ответственности за нарушение норм, регулирующих обработку и обеспечение безопасности ПДн.

Организация в ходе своей деятельности предоставляет доступ к ПДн третьим сторонам в целях исполнения договорных обязательств перед субъектами ПДн, а также с целью обеспечения своей деятельности или исполнения требований нормативных документов РФ. Такой доступ может быть предоставлен третьим сторонам только после подписания соглашения о неразглашении персональных данных (если обязанность третьего лица по соблюдению конфиденциальности персональных данных заранее не установлена нормативными документами РФ).

Права доступа к персональным данным в Организации предоставляется на постоянной или временной основе. Право доступа к персональным данным на постоянной основе имеют работники Организации, непосредственно занимающиеся обработкой ПДн. Основанием для оформления работнику временного (разового) права доступа к ПДн является выполнение производственного задания, в рамках которого работнику объективно необходим доступ к ПДн.

Доступ работников Организации к обработке ПДн осуществляется после:

- ознакомления с положениями законодательства Российской Федерации о персональных данных, документами Организации, устанавливающими порядок обработки и обеспечения безопасности персональных данных, а также об их правах и обязанностях в этой области;
- прохождения внутреннего обучения (инструктажа) по правилам обработки и обеспечения безопасности ПДн;
- ознакомления с эксплуатационной документацией к средствам защиты информации, применяемым в рамках системы защиты персональных данных;
- ознакомления с ответственностью за нарушение установленных в Организации правил обработки и обеспечения безопасности ПДн.

Доступ работников Организации к ИСПДн ограничен системой разграничения прав доступа, реализуемой в рамках системы защиты персональных данных с использованием технических и организационных мероприятий. Каждый пользователь имеет индивидуальную учетную запись, которая определяет его права и полномочия в ИСПДн. Информация об учетной записи не может быть передана другим лицам.

Пользователь несет персональную ответственность за конфиденциальность сведений собственной учетной записи. Запрещается использование для доступа к ИСПДн учетных записей других пользователей. Заведение, активацию, блокирование и уничтожение учетных записей пользователей ИСПДн осуществляет Администратор ИСПДн, который назначается приказом директора Организации. Все работники, допущенные к обработке ПДн, обязаны соблюдать конфиденциальность ПДн как в течение

срока действия трудового договора, так и после его прекращения в течение срока, установленного соглашением о неразглашении персональных данных.
8.2. Изменение прав доступа к персональным данным.

Основанием для изменения прав доступа работника к ПДн является:

- перевод работника на должность, функциональные обязанности которой требуют расширения или сокращения прав доступа к ПДн;
- изменение процесса (процессов) обработки ПДн в Организации и/или требований законодательства РФ в области обработки и обеспечения безопасности ПДн, при которых расширяются или сокращаются права доступа к ПДн, закрепленные за определенными должностями работников;
- изменения в организационно-штатной структуре Организации;
- служебная необходимость, в рамках которой работнику требуется временное (разовое) расширение прав на обработку ПДн;
- проведение в отношении работника служебного расследования, в рамках которого такому работнику необходимо ограничить права доступа к ПДн.

8.3 Прекращение прав доступа к персональным данным.

Основанием для прекращения прав доступа работника к ПДн является:

- нарушение работником требований законодательства Российской Федерации о персональных данных, локальных актов Организации в области обработки и обеспечения безопасности ПДн;
- перевод работника на другую должность или в другое структурное подразделение, не требующих участия в процессах обработки ПДн;
- достижение заявленных целей, для которых работнику предоставлялся временный (разовый) доступ к ПДн; - прекращение трудовых отношений с работником.

9. Предоставление персональных данных третьей стороне.

Предоставление ПДн третьим сторонам осуществляется только с предварительного письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных законодательством Российской Федерации, в частности Федеральным законом «Об обязательном пенсионном страховании в Российской Федерации, Федеральным законом «Об основах обязательного социального страхования, Федеральным законом «Об обязательном медицинском страховании в Российской Федерации». Существенным условием договоров с третьими сторонами, в рамках исполнения которых передаются ПДн, является обязанность соблюдения сторонами мер обеспечения безопасности ПДн при их обработке. Кроме того, в договорах в обязательном порядке определяется порядок передачи ПДн.

Организация с согласия субъекта может поручать обработку ПДн третьим б сторонам, а также выступать в роли лица, осуществляющего работку ПДн по поручению других операторов ПДн.

В случае если Организация поручает обработку третьей стороне, в поручении на обработку ПДн должны быть в обязательном порядке определены:

- перечень действий (операции) с персональными данными, которые будут совершаться третьей стороной;
- цели обработки (цели не должны противоречить целям, заявленным перед субъектом в договоре с оператором, в согласии и т. д.);
- обязанность третьей стороны соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;
- требования к защите ПДн. При обработке ПДн по поручению третьих сторон Организацией соблюдаются установленные соответствующими поручениями (договорами) требования к обеспечению безопасности ПДн.

Федеральным законом может устанавливаться обязанность Организации непосредственно направлять информацию, содержащую ПДн, третьим лицам (отчетность, налоговые декларации и т.д.) либо право третьих лиц запрашивать указанную информацию в пределах их полномочий. В последнем случае передача информации осуществляется на основании письменных мотивированных запросов, оформленных на официальных бланках за подписью уполномоченного должностного лица.

Запрос должен содержать цели и правовые основания затребования информации, срок предоставления такой информации, если иное не установлено законом.

Ответы на запросы направляются законным получателям ПДн только в письменном виде и только в затребованном объеме. Получателями ПДн на законном основании, в том числе являются:

- Фонд социального страхования РФ;
- Пенсионный фонд РФ;
- Федеральная Налоговая Служба;
- Федеральная инспекция труда;
- иные органы надзора и контроля за соблюдением законодательства о труде;
- правоохранительные и судебные органы.

Организация обязана предоставить персональные данные по письменному запросу субъекта персональных данных или его законного представителя. Копии документов, содержащих ПДн, выдаются Организацией в срок не позднее тридцати дней со дня подачи письменного заявления об их выдаче. При выдаче документов для ознакомления, а также запрашиваемых копии и справок, работник, занимающийся обработкой ПДн, обязан удостовериться в личности запрашивающего (или его представителя) и потребовать предоставление документа, подтверждающего соответствующие полномочия.

10. Обращение с материальными носителями персональных данных.

10.1. Виды носителей Персональные данные в Организации хранятся на материальных носителях двух видов:

- машинные (электронные) носители персональных данных;
- бумажные носители персональных данных.

Организация обработки поступивших и создаваемых документов, содержащих персональные данные, осуществляется в соответствии с принятыми в Организации нормами документооборота.

10.2. Хранение бумажных носителей персональных данных Бумажные (документальные) носители ПДн должны храниться в Организации, исключающих несанкционированный доступ в них посторонних лиц, в сейфах или запираемых металлических шкафах (ящиках).

Хранение бумажных (документальных) носителей ПДн вместе документами общего доступа запрещается, за исключением случаев, когда документы общего доступа являются приложениями к бумажным (документальным) носителям ПДн.

Запрещается совместное хранение бумажных (документальных) носителей ПДн, обработка которых осуществляется в различных целях. Для каждой категории персональных данных должны быть определены и занесены в Реестр места хранения бумажных носителей этой категории.

В Реестре мест хранения носителей персональных данных указывают:

- наименование процесса, цели обработки и категории субъектов персональных данных; - категории персональных данных;
- место хранения (номер или наименование помещения, в котором хранятся бумажные носители, номер шкафа (сейфа) в котором хранятся бумажные носители);
- перечень документов;
- перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

10.3. Уничтожение бумажных носителей персональных данных Основанием для уничтожения бумажных (документальных) носителей ПДн является:

- достижение целей обработки, в том числе истечение сроков обязательного хранения, установленных законодательством РФ;
- отзыв согласия субъекта на обработку его ПДн;
- получение соответствующего запроса от субъекта ПДн;
- получение соответствующего указания от уполномоченного органа по защите прав субъектов. Уничтожение бумажных (документальных) носителей ПДн производится способом, исключающим возможность восстановления информации.

10.4. Использование и обеспечение сохранности машинных носителей персональных данных Для обработки (хранения) персональных данных в информационных системах персональных данных Организации используются машинные носители, в роли которых могут выступать неотчуждаемые носители (жесткие диски) или отчуждаемые (съемные) носители информации (такие как: внешние жесткие диски, гибкие магнитные

диски, USB флэш – накопители, карты флэш-памяти, оптические носители и др.).

В целях предотвращения нарушения целостности и утери персональных Данных, обрабатываемых в информационных системах персональных данных Организации, пользователь ИСПДн должен осуществлять резервное копирование необходимой информации по мере ее обновления на отчуждаемые (съемные) носители информации.

Для обеспечения сохранности машинных носителей должен быть организован режим обеспечения безопасности помещений, в которых размещены технические средства информационных систем персональных данных, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

Системные блоки с жесткими дисками, на которых хранятся персональные данные должны быть опечатаны лицом ответственным за организацию обработки персональных данных. Хранение отчуждаемых (съемных) носителей персональных данных должно осуществляться в сейфах или запираемых металлических шкафах (ящиках). Несанкционированный вынос машинных носителей из Организации запрещен.

10.5. Учет машинных носителей персональных данных.

Все машинные носители, используемые для обработки и хранения персональных данных, регистрируются и учитываются в Журнале учета машинных носителей персональных данных (далее - Журнал).

В Журнале указывают: — Ф.И.О. работника; — Дата получения и подпись работника; — Номер машинного носителя; — Тип носителя; — Дата возврата и подпись работника; — Отметка об уничтожении; — Дата уничтожения и подпись Администратора ИСПДн. Ответственность за ведение Журнала несут Администраторы ИСПДн.

10.6. Уничтожение машинных носителей персональных данных В случае выхода из строя или принятия решения о прекращении использования машинного носителя в процессах обработки персональных данных такой носитель уничтожается или с него стираются персональные данные (способом исключающим возможность восстановление данных).

11. Защита персональных данных.

11.1. Общие положения Защита персональных данных представляет собой комплекс мер технического, организационного и организационно - технического характера, направленных на обеспечение конфиденциальности, целостности и доступности ПДн.

Организация при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокировании, копирования, предоставления, распространения персональных

данных, а также от иных неправомерных действий в отношении персональных данных. К таким мерам в частности, относятся:

- назначение лица, ответственного за организацию обработки персональных данных;
- осуществление внутреннего контроля за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- ознакомление работников Оператора с положениями законодательства Российской Федерации о персональных данных, локальными актами по вопросам обработки персональных данных, требованиями к защите персональных данных;
- издание локальных актов по вопросам обработки персональных данных и локальных актов, устанавливающих процедуры, направленные на предотвращение и выявления нарушений законодательства РФ;
- определение угроз безопасности персональных данных и необходимого уровня защищённости персональных данных, при их обработке в информационных системах персональных данных;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;
- осуществление оценки эффективности применяемых мер по обеспечению безопасности персональных данных.

В Организации защите подлежат: - документы на бумажных носителях, содержащие персональные данные;

- персональные данные в электронном виде, обрабатываемые в информационных системах персональных данных.

При обработке ПДн в информационных системах персональных данных их защита осуществляется с учетом положений документа «Требования к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Постановлением Правительства РФ от 1 ноября 2012 г. № 1119). Для каждой ИСПДн Организации должна быть разработана Модель угроз и определен требуемый уровень защищенности персональных данных при их обработке в ИСПДн. При обработке ПДн без использования средств автоматизации (на бумажных носителях) защита персональных данных осуществляется с учетом требований нас настоящего Положения «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (утв. Постановлением Правительства РФ от 15.09.2008 № 687).

Все работники Организации, участвующие в обработке ПДн, в обязательном порядке должны проходить инструктаж по следующим

направлениям: - общие вопросы обеспечения информационной безопасности в Организации; - правила обработки ПДн; - правила использования средств защиты информации; - ответственность за нарушение правил обработки и обеспечения безопасности ПДн.

11.2. Система защиты персональных данных. Обеспечение безопасности персональных данных при их обработке в ИСПДн Организации обеспечивается с помощью системы защиты персональных данных (далее - СЗПДн).

Объектами защиты ИСПДн являются персональные данные, содержащиеся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители персональных данных, средства и системы связи и передачи данных), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

Цель реализации СЗПДн - защита ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении ПДН.

СЗПДн включает в себя организационные и технические меры, определенные с учетом актуальных для ИСПДн угроз безопасности персональных данных и информационных технологий, используемых в ИСПДн.

Целью реализации в СЗПДн технических мер является обеспечение конфиденциальности, целостности и доступности ПДн в процессе их обработки и хранения в ИСПДн, предотвращение утечки и НСД к ПДн при их обработке в ИСПДн.

В рамках технических мер - в составе СЗПДн используются средства защиты информации, сертифицированные по требованиям безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Целями организационных мероприятий по защите ПДн в Организации являются:

- исключение непреднамеренных действий работников Организации, приводящих к утечке, искажению, уничтожению ПДн, в том числе ошибки эксплуатации ИСПДн;

- сведение к минимуму возможности нарушения свойств безопасности ПДн с помощью любых средств, не связанных непосредственно с эксплуатацией ИСПДн (физический вынос ПДн на машинных носителях);

- исключение ознакомления работников с ПДн, если это не предусмотрено их должностными обязанностями.

В рамках мер физической защиты - в соответствии с установленным порядком пропускного и внутриобъектового режима в Организации, для обеспечения безопасности ПДн применяются следующие меры и средства:

- организация режима обеспечения безопасности помещений, в которых размещены технические средства ИСПДн, препятствующего

возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- системы пожарной сигнализации и пожаротушения;

- исключение возможности просмотра неуполномоченными лицами текстовой и графической информации, содержащей персональные данные, с устройств отображения информации (мониторов).

Разработка СЗПДн и ее внедрение (в том числе внедрение средств защиты информации) осуществляется в соответствии с положениями Приказа ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Для осуществления мероприятий по разработке и внедрению СЗПДн на договорной основе может привлекаться организация, имеющая лицензию на осуществление деятельности по технической защите конфиденциальной информации. Результаты разработки СЗПДн отражаются в Описании системы защиты персональных данных. Результаты внедрения СЗПДн отражаются в Техническом паспорте ИСПДн.

11.3. Оценка эффективности применяемых мер по обеспечению безопасности персональных данных.

Оценка эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности ПДн проводится Организацией самостоятельно или с привлечением на договорной основе организации, имеющей лицензию на осуществление деятельности по технической защите конфиденциальной информации. Оценка эффективности может проводится в форме декларирования соответствия или в рамках работ по аттестации информационной системы персональных данных в соответствии с национальным стандартом ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

12. Права субъектов персональных данных Права субъектов персональных данных (либо их законных представителей) определены в Политике Организации в отношении обработки персональных данных и положениях законодательства Российской Федерации в области обработки персональных данных.

13. Роли в области организации обработки и обеспечения безопасности персональных данных

13.1. Перечень ролей В целях обеспечения законного порядка обработки и обеспечения безопасности ПДн в Организации выделяются следующие роли Ответственный за организацию обработки персональных данных:

- работник Организации, осуществляющий организацию выполнения требований законодательства Российской Федерации при обработке и обеспечении безопасности ПДн в Организации; Администратор ИСПДн;

- работник Организации, обеспечивающий бесперебойное функционирование информационной системы персональных данных;

Пользователь работник Организации, непосредственно осуществляющий обработку ПДн.

13.2. Права и обязанности Ответственного за организацию обработки персональных данных Ответственный за организацию обработки ПДн обязан:

- осуществлять внутренний контроль за соблюдением Организацией и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных (пункт 1 часть 4 ст.22.1. 152-ФЗ);
- доводить до сведения работников Организации положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных (пункт 2 часть 4 ст. 22.1 152-ФЗ);
- организовывать (обеспечивать) прием и обработку обращений и запросов субъектов персональных данных (пункт 3 часть 4 ст. 22.1 1 52-ФЗ);
- организовывать построение и эксплуатацию СЗПДн Организации и, при необходимости ее модернизацию;
- обеспечивать поддержание в актуальном состоянии организационно-распорядительных документов Организации по организации обработки и обеспечению безопасности ПДн;
- проводить систематический контроль за выполнением комплекса организационно- технических мероприятий по организации обработки и обеспечению безопасности персональных данных, в том числе за выполнением Администратором ИСПДн своих обязанностей;
- хранить дистрибутивы программного обеспечения средств защиты информации ИСПДн, а также эксплуатационную документацию и сертификаты средств защиты информации;
- организовывать проведение инструктажей и обучения работников Организации по вопросам обработки и обеспечения безопасности персональных данных;
- осуществлять взаимодействие с регулирующими органами по вопросам обработки и обеспечения безопасности ПДн, в том числе координировать действия работников Организации при проведении проверок регулирующими органами, а также при обработке запросов указанных органов;
- предоставлять консультации и оказывать содействие работникам Организации по вопросам обработки и обеспечения безопасности персональных данных в рамках своей компетенции;
- незамедлительно принимать меры пресечения и уведомлять руководителя Организации в случае обнаружения попыток или фактов несанкционированного доступа к ПДн, а также нарушения требований организационно-распорядительных документов Организации по организации обработки и обеспечению безопасности ПДн.

Ответственный за организацию обработки ПДн имеет право:

- давать указания Администратору ИСПДн и контролировать их выполнение;

- вносить предложения по совершенствованию процессов обработки и обеспечения безопасности персональных данных в Организации;

- требовать от работников устранения выявленных нарушений и предоставления письменных объяснений по фактам нарушений требований организационнораспорядительных документов Организации по организации обработки и обеспечению безопасности ПДн;

- запрашивать у работников, участвующих в процессах обработки и обеспечения безопасности ПДн, информацию и документы, необходимые для выполнения функциональных обязанностей.

13.3. Права и обязанности Администратора ИСПДн.

Администратор ИСПДн обязан:

- обеспечивать настройку и бесперебойную эксплуатацию программных и технических средств обработки ПДн, входящих в состав ИСПДн Организации;
- обеспечивать настройку, бесперебойную эксплуатацию и мониторинг средств защиты информации, входящих в состав СЗПДн Организации;
- настраивать права доступа работников к персональным данным и средствам их обработки в Организации в соответствии с ролевой моделью доступа;
- проводить инструктаж пользователей ИСПДн по правилам эксплуатации программных и технических средств обработки ПДн, входящих в состав ИСПДн Организации и средств защиты информации, входящими в состав СЗПДн Организации;
- контролировать смену паролей пользователями ИСПДн не реже одного раза в три месяца либо при компрометации паролей;
- организовать учет, хранение и уничтожение машинных носителей персональных данных;
- хранить дистрибутивы программного обеспечения средств обработки информации ИСПДн;
- обеспечивать контроль сторонних организаций (подрядчиков), при привлечении последних для обслуживания, настройки и ремонта средств обработки и защиты информации ИСПДн;
- предоставлять необходимую информацию при проведении проверок регулирующими органами, а также проведении контрольных мероприятий по обеспечению безопасности ПДн;
- предоставлять консультации и оказывать содействие работникам, участвующим в процессах обработки и обеспечения безопасности ПДн, по вопросам использования средств обработки информации ИСПДн, в рамках своей компетенции;
- в случае обнаружения попыток или фактов несанкционированного доступа к ПДн, незамедлительно уведомлять о выявленных фактах Ответственного за организацию обработки ПДн.

Администратор ИСПДн имеет право:

- вносить предложения по совершенствованию ИСПДн и СЗПДн Организации, в том числе организационно-распорядительных документов в области обработки и обеспечения безопасности ПДн;

- запрашивать у работников, участвующих в процессах обработки и обеспечения безопасности ПДн, информацию и документы, необходимые для выполнения функциональных обязанностей.

13.4 Права и обязанности Пользователя.

Пользователь обязан:

- строго соблюдать положения законодательства РФ о персональных данных, локальных актов Организации по вопросам обработки персональных данных, требований к защите персональных данных. Пользователь имеет право:

- запрашивать у лица ответственного за организацию обработки персональных данных разъяснения положений законодательства РФ о персональных данных, локальных актов Организации по вопросам обработки персональных данных, требований к защите персональных данных;

- вносить предложения по совершенствованию процессов обработки и обеспечения безопасности персональных данных в Организации.

- запрашивать у работников, участвующих в процессах обработки и обеспечения безопасности ПДн, информацию и документы, необходимые для выполнения функциональных обязанностей.

14. Ответственность.

14.1. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных Лица, виновные в нарушении норм, регулирующих обработку ПДн, несут дисциплинарную, административную, гражданскую, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.

Прекращение доступа к персональным данным и/или увольнение не освобождает работника Организации от принятых обязательств по неразглашению персональных данных, ставших доступными при выполнении должностных обязанностей.

К административной ответственности за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах и за нарушение правил защиты информации могут привлекаться как сама Организация и его должностные лица, так и конкретные работники, исполняющие соответствующие трудовые функции.

14.2. Описание видов ответственности.

Виды дисциплинарных взысканий, порядок их применения и снятия установлены главой 34 ТК РФ и Правилами внутреннего трудового распорядка Организации.

Порядок защиты нематериальных благ, к числу которых относятся честь и доброе имя, деловая репутация;

-неприкосновенность частной жизни; личная и семейная тайна определяется Гражданским кодексом РФ и иными законами. Лица, виновные

в нарушении правил работы с ПДн, могут привлекаться к административной ответственности в частности по следующим основаниям:

- неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих его права и свободы, либо несвоевременное предоставление таких документов и материалов, непредоставление иной информации в случаях, предусмотренных законам, либо предоставление гражданину неполной или заведомо недостоверной информации (ст. 5.39 КоАП);

- нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11 КоАП); - нарушение правил защиты информации (ст. 13.12 КоАП);

- разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, когда ее разглашение влечет уголовную ответственность), лицом, получившим к ней доступ в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14 КоАП РФ).

Уголовная ответственность за нарушение правил работы с ПДн может наступить в частности в следующих случаях:

- незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан (ст. 137 УК РФ);

- неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан (ст. 140 УК РФ);

- неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (ст. 272 УК РФ);

- нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационнотелекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб или повлекшее тяжкие последствия (ст.274 УК РФ).

Приложение № 9
к Приказу № 117 от 03.09.2018г.

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных (ИСПДн) в МБДОУ ДС №48 «Одуванчик» г.Светлоград

1. Общие положения

1.1. Пользователь информационных систем персональных данных (ИСПДн) (далее - Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.
1.2. Пользователем является каждый сотрудник МБДОУ ДС № 48 «Одуванчик» г. Светлоград, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
1.3. Пользователь несет персональную ответственность за свои действия.
1.4. Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами МБДОУ ДС № 48 «Одуванчик» г.Светлоград. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных. вопросам информационной безопасности, необходимо обратиться в администрацию детского сада.
1.5 Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн. Пользователям запрещается:
- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения своего руководителя;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции;
- запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

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

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

2.Организация парольной защиты

2.1.Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором информационной безопасности, Администратором ИСПДн. - запрещается нецелевое использование подключения к Сети.

3.Права и ответственность пользователей ИСПДн

3.1.Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.
3.2.Пользователи, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N152-ФЗ "О персональных данных" и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

4. Должностные обязанности

Пользователь обязан:

4.1.Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

4.2.Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.

5. Правила работы в сетях общего доступа и (или) международного обмена.

5.1.Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее - Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

5.2.При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- запрещается скачивать из Сети программное обеспечение и другие файлы;
- запрещается посещение сайтов сомнительной репутации (порно- сайты, сайты, содержащие нелегально распространяемое ПО и другие).

Приложение № 10
к Приказу № 117 от 03.09.2018г.

ИНСТРУКЦИЯ
по антивирусной защите в информационных системах МБДОУ ДС №48 «Одуванчик» г. Светлоград

1 Общие положения

1.1 Настоящая Инструкция предназначена для всех сотрудников МБДОУ ДС №48 «Одуванчик» г. Светлоград (далее – ДОУ), имеющих доступ к информационным системам (ИС) ДОУ.

1.2 Инструкция устанавливает требования и ответственность при организации защиты информации от воздействия вредоносных компьютерных вирусов.

1.3 Инструкция регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля при работе в ИС ДОУ

2 Обеспечение антивирусной защиты

2.1 Порядок организации антивирусной защиты.

2.1.1 Для организации антивирусной защиты ИС ДОУ допускаются к использованию только сертифицированные ФСТЭК России лицензионные антивирусные средства общего применения.

2.1.2 Антивирусное средство защиты должно быть установлено на все средства вычислительной техники (СВТ) (при наличии технической возможности), входящие в ИС ДОУ.

2.1.3 В ИС ДОУ права по управлению (администрированию) средствами антивирусной защиты предоставлены только администратору информационной безопасности.

2.1.4 Разработка и осуществление мероприятий по проведению антивирусного контроля осуществляется ответственным за защиту информации с привлечением (при необходимости) администратора информационной безопасности и /или специалистов лицензированной организации.

2.1.5 Должностные лица не должны допускать использования в ДОУ программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

2.1.6 В ИС ДОУ обеспечивается централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (автоматизированных рабочих местах).

2.1.7 В ИС ДОУ обеспечивается централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов).

2.1.8 Расширенный антивирусный контроль проводится администратором информационной безопасности не реже одного раза в месяц и при необходимости, в случае подозрений в заражении вирусной программой.
2.1.9 При загрузке, открытии или исполнении объектов (файлов) из внешних источников средствами антивирусной защиты проводится автоматическая проверка объектов (файлов).
2.1.10 В виртуальной инфраструктуре обеспечивается реализация и управление антивирусной защитой:
2.1.10.1 проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;
2.1.10.2 проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.
2.2 Порядок проведения антивирусного контроля.
2.2.1 Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется администратором информационной безопасности на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, должна быть выполнена антивирусная проверка администратором информационной безопасности.
2.2.2 При загрузке компьютера средствами антивирусной защиты проводится антивирусный контроль в автоматическом режиме.
2.2.3 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИС ДОУ самостоятельно или вместе с администратором информационной безопасности проводит внеочередной антивирусный контроль своей рабочей станции для определения факта наличия или отсутствия компьютерного вируса.
2.2.4 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИС ДОУ обязаны:
- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и администратора информационной безопасности, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на съемном носителе информации администратору информационной

безопасности для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при наличии);
- по факту обнаружения зараженных вирусом файлов составить служебную записку администратору информационной безопасности, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.
2.3 Обновление базы данных признаков вредоносных компьютерных программ (вирусов).
2.3.1 Администратор информационной безопасности обеспечивает получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов).
2.3.2 Контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов) обеспечивается путем автоматического получения или предварительно скачиваемых обновлений из официальных источников, например, с сервера обновлений производителя антивирусного средства.

3 Ответственность при организации антивирусной защиты

3.1 Ответственность за организацию антивирусной защиты ИС ДОУ в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.
3.2 Ответственность за соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности, администратора ИС ДОУ, администратора виртуальной инфраструктуры и пользователей, эксплуатирующих ИС ДОУ.

Приложение № 11
к Приказу № 117 от 03.09.2018г.

ИНСТРУКЦИЯ
администратора безопасности информации в МБДОУ ДС №48 «Одуванчик» г. Светлоград

1. Общие положения

Данная Инструкция является руководящим документом администратора безопасности информации в МБДОУ ДС №48 «Одуванчик» г.Светлоград далее (ДОУ) Требования настоящей инструкции должны выполняться во всех режимах функционирования.

Требования администратора безопасности, связанные с выполнением им своих функций, обязательны для исполнения всеми сотрудниками. Персональные данные относятся к категории информации ограниченного распространения.

Наиболее вероятными каналами утечки информации для информационных систем персональных данных (ИСПДн) являются:

- несанкционированный доступ к информации, обрабатываемой в ИСПДн;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

Работа с персональными данными (ПДн) строится на следующих принципах:

- принцип персональной ответственности – в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник, выдача документов осуществляется только под роспись;
- принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

1.1. Назначение администратора безопасности.

На должность администратора безопасности назначается лицо из числа наиболее квалифицированных пользователей ПЭВМ, либо имеющим образование в области защиты информации, в котором эксплуатируется информационная система. Администратор безопасности в вопросах защиты

информации взаимодействует с сотрудниками отдела по защите информации Правительства края.

2.Обязанности администратора безопасности структурного подразделения.

В своей повседневной деятельности администратор руководствуется данной инструкцией и другими документами, регламентирующими защиту персональных данных от утечки по техническим каналам и НСД, эксплуатационной документацией на установленные на объекте информатизации системы защиты от несанкционированного доступа к информации (СЗИ НСД) и от утечки информации по техническим каналам.

Администратор безопасности совместно со специалистами по информационным технологиям и защите информации:

- обеспечивает поддержку подсистем управления доступом, регистрации и учета информационных ресурсов;
- контролирует целостность программно-аппаратной среды, хранимой и обрабатываемой информации;
- контролирует доступность и конфиденциальность хранимой, обрабатываемой и передаваемой по каналам связи информации (устойчивое функционирование ЛВС и ее подсистем).

На администратора безопасности возлагаются следующие обязанности:

- следить за сохранностью наклеек с защитной и идентификационной информацией на корпусах ПЭВМ;
- знать уровень конфиденциальности обрабатываемой информации и класс ИСПДн, следить за тем, чтобы обработка информации производилась только с использованием учтенных съемных и несъемных носителей информации;
- контролировать соблюдение требований по учету и хранению носителей конфиденциальной информации и персональных данных;
- совместно со специалистами по информационным технологиям и защите информации обеспечивать доступ к защищаемой информации пользователям согласно их прав доступа;
- незамедлительно докладывать руководителю учреждения, обо всех выявленных попытках несанкционированного доступа к информации ограниченного доступа;
- контролировать правильность применения пользователями сети средств защиты информации;
- участвовать в испытаниях и проверках ИСПДн;
- не допускать к работе на рабочих станциях и серверах посторонних лиц;
- осуществлять контроль монтажа оборудования специалистами сторонних организаций;
- участвовать в приемке для нужд новых программных средств;

- обобщать результаты своей деятельности и готовить предложения по ее совершенствованию;

- при изменении конфигурации автоматизированной системы вносить соответствующие изменения в паспорт ИСПДн, обрабатывающей информацию ограниченного доступа;

- вести журнал учета работы с ИСПДн. Регистрации в журнале учета работ ИСПДн подлежат:

- обновление программного обеспечения ИСПДн;

- обновление антивирусных баз; - вскрытие системного блока с целью модернизации или ремонта с указанием цели вскрытия и проводимых работ;

- создание резервной копии базы данных и пр. служебной информации;

- замена системного блока с указанием факта гарантированного удаления информации с жесткого магнитного диска;

- отклонения в нормальной работе системных и прикладных программных средств затрудняющих эксплуатацию рабочей станции;

- выход из строя или неустойчивое функционирование узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.);

- перебои в системе электроснабжения;

- и.т.п.

При выявлении нарушения первой категории (утечка информации) администратор обязан немедленно прекратить работы в ИСПДн.

При выявлении нарушений первой, второй и третьей категорий администратор обязан подать служебную записку руководству и занести соответствующую запись в журнал учета работы ИСПДн с изложением факта нарушения, предпринятые и/или рекомендуемые им действия.

Форма журнала регистрации работ ИСПДн:

Дата	Наименование работ	Ф.И.О. исполнителя работ	ИСПДн _____	Роспись
1	2	3	4	5

3.Ответственность.

Администратор безопасности несет всю полноту ответственности за качество и своевременность выполнения задач и функций, возложенных на его в соответствии с настоящей Инструкцией и другими нормативными документами по защите информации.