

ПРИНЯТО

На общем собрании работников МАДОУ
Детский сад № 15 «Сказка»
Протокол № 3 от 04.03.2025.

УТВЕРЖДАЮ
Заведующий МАДОУ детский сад № 15
«Сказка»

Л.В.Галимуллина

Приказ № 17 от 04.03.2025

ИНСТРУКЦИЯ

по порядку учета, хранения и уничтожения персональных данных
в муниципальном бюджетном дошкольном образовательном учреждении
детском саду № 15 «Сказка» города Благовещенска Республики
Башкортостан

1. Определения

- 1.1. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.
- 1.2. Администратор безопасности информации – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системой защиты информации в соответствии с установленной ролью.
- 1.3. Безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.
- 1.4. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
- 1.5. Доступность информации (ресурсов информационной системы) – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.
- 1.6. Защищаемая информация – информация, для которой обладателем информации определены характеристики ее безопасности.
- 1.7. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
- 1.8. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
- 1.9. Информация – сведения (сообщения, данные) независимо от формы их представления.
- 1.10. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
- 1.11. Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

- 1.12. Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.
- 1.13. 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.
- 1.14. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
- 1.15. Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.
- 1.16. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
- 1.17. Средство защиты информации – техническое, программное, программно-техническое средство, предназначенное или используемое для защиты информации.
- 1.18. Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

2. Общие положения

- 2.1. Настоящая Инструкция разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 6 марта 1997 года №188 «Об утверждении перечня сведений конфиденциального характера», Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- 2.2. Настоящая Инструкция устанавливает порядок работы с документами – носителями конфиденциальной информации, содержащей персональные данные, в информационных системах обрабатывающих информацию организации доступа в муниципальном автономном дошкольном образовательном учреждении детский сад №15 «Сказка» комбинированного вида г. Благовещенска РБ (далее – Учреждение) в целях:
- предотвращения неконтролируемого распространения конфиденциальной информации, содержащей персональные данные в результате ее разглашения должностным лицом, имеющим доступ к информации, содержащей персональные данные, или получения несанкционированного доступа к конфиденциальной информации;
 - предотвращения несанкционированного уничтожения, искажения, копирования, блокирования информации, содержащей персональные данные;
 - предотвращения утраты, несанкционированного уничтожения или сбоев в

процессе функционирования автоматизированных систем обработки информации, содержащей персональные данные, обеспечение полноты, целостности, достоверности такой информации;
соблюдения правового режима использования информации, содержащей персональные данные;
обеспечения возможности обработки и использования персональных данных Учреждения, его структурными подразделениями и должностными лицами, имеющими соответствующие полномочия.

3. Хранение и уничтожение персональных данных

- 3.1. Персональные данные субъекта ПДн хранятся в подразделении Учреждения, которое осуществляет их обработку и отвечает за взаимодействие с субъектом персональных данных.
- 3.2. ПДн на бумажном носителе хранятся в папках в сейфе или в шкафу, имеющем замки, которые закрываются на ключ.
- 3.3. Персональные данные субъекта ПДн в электронном виде хранятся в локализованных электронных базах данных компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные субъекта, обеспечиваются системой защиты информации.
- 3.4. В нерабочее время помещение, где хранятся ПДн (хранилище ПДн), должно закрываться на ключ. В рабочее время, в случае ухода руководителя, помещение должно быть закрыто на ключ или оставлено под ответственность лиц, назначенных директором Учреждения.
- 3.5. Сотрудник организации, имеющий доступ к персональным данным субъектов ПДн, в связи с исполнением трудовых обязанностей, обеспечивает хранение информации, содержащей персональные данные субъекта, исключая доступ к ним третьих лиц.
- 3.6. В отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные субъектов (соблюдение «политики чистых столов»).
- 3.7. При уходе в отпуск, нахождении в служебной командировке и иных случаях длительного отсутствия сотрудника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные субъектов ПДн лицу, на которое приказом будет возложено исполнение его трудовых обязанностей.
- 3.8. В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные субъектов ПДн по указанию директора Учреждения, передаются другому сотруднику, имеющему доступ к персональным данным субъектов ПДн.
- 3.9. При увольнении сотрудника, имеющего доступ к персональным данным субъектов ПДн, документы и иные носители, содержащие персональные данные субъектов ПДн, по приказу заведующего Учреждения передаются другому сотруднику, имеющему доступ к персональным данным субъектов ПДн.
- 3.10. Повседневный контроль за выполнением требований по защите хранилищ ПДн осуществляют лица, ответственные за помещение (хранилище ПДн).
- 3.11. Периодический контроль эффективности мер защиты хранилищ ПДн осуществляется ответственным за организацию обработки и обеспечение защиты персональных данных.
- 3.12. Уничтожение персональных данных субъектов ПДн на бумажном

носителе, либо удаление электронных баз данных, содержащих персональные данные субъектов ПДн в электронном виде, осуществляется по истечении установленного срока обработки ПДн комиссией, назначенной приказом Учреждения.

4. Порядок предоставления доступа к персональным данным

4.1. Основанием для допуска сотрудника к работе с персональными данными является включение его в список лиц, допущенных к обработке персональных данных. Включение в список лиц, допущенных к работе с персональными данными, осуществляется приказом заведующего Учреждения по представлению ответственного лица за обеспечение безопасности информации. При допуске к работе с персональными данными определяется перечень информационных систем персональных данных, к работе в которых допущен работник Учреждения, а также перечень обрабатываемых им персональных данных и разрешенный вид процедур обработки ПДн.

4.2. Доступ к персональным данным имеют сотрудники Учреждения, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей согласно перечню должностей, указанных в приложении 2 к настоящему приказу.

4.3. Пользователи допускаются к работе с ресурсами ИС только после прохождения инструктажа, проводимого ответственным лицом за безопасность информации и ознакомление с требованиями Политики в области организации обработки и обеспечения безопасности ПДн, должностной инструкции и иными локальными нормативными актами Учреждения в сфере обеспечения безопасности персональных данных.

4.4. Основанием для прекращения допуска сотрудника к работе с персональными данными или внесение изменений в его обязанности по работе в информационной системе, внесению изменений в перечень обрабатываемых ПДн и перечень процедур обработки ПДн является приказ заведующего Учреждения.

4.5. Внесение предложений на утверждение директору Учреждения по изменению списка лиц, допущенных к работе с персональными данными, осуществляется ответственным лицом за обеспечение безопасности информации.

5. Порядок обеспечения безопасности персональных данных

5.1. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых без использования средств автоматизации утвержден в «Положении о порядке обработки персональных данных без использования средств автоматизации».

5.2. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых с использованием средств автоматизации утвержден в Правилах обработки персональных данных субъектов персональных данных.

3.3. Порядок учёта, хранения и обращения со съёмными носителями персональных данных утвержден в «Инструкции по порядку учёта, хранения и уничтожения машинных носителей информации».

6. Ответственность

6.1. Работники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательстве.