Муниципальное бюджетное дошкольное образовательное учреждение Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово»

ПРИКАЗ

09 сентября 2022 года **№ 95**

д. Денисово

Об утверждении инструкций по обеспечению безопасности персональных данных и функционированию информационных систем

В целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

П Р И К А З Ы В А Ю:

1. Утвердить:

1) Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах (приложение №1).

2) Инструкцию администратора безопасности системы защиты персональных данных информационной системы (приложение №2).

3) Инструкцию пользователя информационной системы (приложение №3).

4) Инструкцию по организации резервного копирования и восстановления персональных данных в информационной системе (приложение №4).

5) Инструкцию по организации учета, использования и уничтожения машинных носителей, предназначенных для обработки и хранения персональных данных в информационной системе (приложение №5).

6) Инструкцию по организации парольной защиты в информационной системе (приложение №6).

7) Инструкцию по применению средств антивирусной защиты информации в информационной системе (приложение №7).

8) Инструкцию по обеспечению защиты информации при выводе из эксплуатации информационной системы (приложение №8).

2. Администратору безопасности обеспечить наличие инструкций на рабочих местах пользователей и проводить инструктаж по правилам работы в информационных системах в соответствии с требованиями инструкций, указанных в п. 1 настоящего приказа.

3. Ответственному за обеспечение безопасности персональных данных в информационных системах обеспечить контроль за выполнением пользователями и администраторами безопасности требований инструкций, указанных в п. 1 настоящего приказа, и своевременным пересмотром инструкций.

4. Контроль исполнения настоящего приказа оставляю за собой.

Заведующий О.В. Лошкарева

УТВЕРЖДАЮ

Заведующий
Муниципальным бюджетным
дошкольным образовательным
учреждением Измалковского
муниципального района Липецкой
области «Детский сад «Сказка»
д. Денисово»
_____ О.В. Лошкарева
«09» сентября 2022 г.

Приложение №1 к Приказу № 95
от «09» сентября 2022 г.

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в информационных системах

1. Общие положения

1.1. Ответственный за обеспечение безопасности персональных данных в информационных системах (далее – Ответственный) в Муниципальном бюджетном дошкольном образовательном учреждении Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» назначается приказом заедующего.

1.2. Ответственный в своей работе руководствуется положениями действующего законодательства о защите персональных данных, настоящей Инструкцией и иными локальными документами Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» по защите персональных данных.

1.3. Настоящая Инструкция определяет основные задачи, обязанности и права Ответственного по вопросам обеспечения защиты персональных данных при их обработке в информационных системах.

2. Основные задачи Ответственного

2.1. Обеспечение безопасности персональных данных в информационных системах.

2.2. Формирование требований к защите персональных данных, содержащихся в информационных системах.

2.3. Разработка систем защиты персональных данных информационных систем.

2.4. Внедрение систем защиты персональных данных.

2.5. Оценка эффективности реализованных в рамках систем защиты персональных данных мер по обеспечению безопасности персональных данных.

2.6. Ввод в эксплуатацию информационных систем.

2.7. Обеспечение защиты персональных данных в ходе эксплуатации информационных систем.

2.8. Обеспечение защиты персональных данных при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки персональных данных.

3. Обязанности Ответственного

Для реализации поставленных задач Ответственный обязан:

3.1. Инициировать создание комиссии для установления уровня защищенности персональных данных при их обработке в информационных системах.

3.2. Совместно с членами комиссии определять уровни защищенности персональных данных при их обработке в информационных системах, и классы защищенности ГИС в отношении которых Муниципальное бюджетное дошкольное образовательное учреждение

Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» является оператором.

3.3. Определять угрозы безопасности персональных данных, реализация которых может привести к нарушению безопасности персональных данных в информационной системе.

3.4. Определять требования к системам защиты персональных данных.

3.5. Определять типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа).

3.6. Определять правила разграничения доступа субъектов доступа к объектам доступа, подлежащие реализации в информационной системе.

3.7. Определять виды и типы средств защиты информации, обеспечивающие реализацию технических мер по обеспечению безопасности персональных данных.

3.8. Выбирать меры по обеспечению безопасности персональных данных, подлежащие реализации в системе защиты персональных данных.

3.9. Определять структуру системы защиты персональных данных информационной системы, включая состав (количество) и места размещения ее элементов.

3.10. Осуществлять выбор средств защиты информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также уровня защищенности персональных данных.

3.11. Определять параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер по обеспечению безопасности персональных данных, а также устранение возможных уязвимостей информационных систем, приводящих к возникновению угроз безопасности персональных данных.

3.12. Осуществлять контроль установки и настройки средств защиты информации в информационных системах.

3.13. Разрабатывать и поддерживать в актуальном состоянии организационно-распорядительные документы, регламентирующие правила и процедуры, реализуемые Муниципальным бюджетным дошкольным образовательным учреждением Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» для обеспечения защиты персональных данных в информационных системах в ходе их эксплуатации (далее – организационно-распорядительные документы по защите персональных данных).

3.14. Обеспечивать внедрение организационных мер по обеспечению безопасности персональных данных.

3.15. Доводить до сведения сотрудников, допущенных к обработке персональных данных в информационных системах, положения организационно-распорядительных документов по защите персональных данных, информировать о политике информационной безопасности в Муниципальном бюджетном дошкольном образовательном учреждении Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» и степени ответственности при работе с защищаемой информацией.

3.16. Присутствовать при проведении предварительных испытаний системы защиты персональных данных.

3.17. Присутствовать при проведении опытной эксплуатации системы защиты персональных данных.

3.18. Присутствовать при проведении приемочных испытаний системы защиты персональных данных.

3.19. Принимать организационные меры по организации безопасности помещений, в которых размещены компоненты информационных систем, препятствующие несанкционированному доступу к персональным данным.

3.20. Осуществлять контроль за размещением устройств вывода (отображения) информации в пределах контролируемой зоны способом, исключающим

несанкционированный просмотр информации ограниченного доступа. При обнаружении данных устройств напротив окон, входных дверей, в коридорах и холлах, изменять расположение устройства или обеспечивать установку дополнительных средств, ограничивающих возможность визуального ознакомления с защищаемой информацией посторонних лиц.

3.21. Организовывать опечатывание корпусов средств вычислительной техники, с которыми осуществляется штатное функционирование СКЗИ, и проводить контроль наличия опечатывающих элементов.

3.22. Осуществлять контроль (анализ) защищенности персональных данных при их обработке в информационных системах, в том числе:

- контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе;
- контроль соблюдения режима защиты персональных данных при их обработке в информационных системах;
- анализ изменения угроз безопасности персональных данных в информационных системах, возникающих в ходе их эксплуатации, и принятие мер по обеспечению безопасности персональных данных в случае возникновения новых угроз безопасности персональных данных;
- контроль наличия и актуальности организационно-распорядительных документов по защите персональных данных;
- документирование процедур и результатов контроля (анализа) защищенности персональных данных при их обработке в информационных системах.

3.23. По результатам контроля (анализа) защищенности персональных данных при их обработке в информационных системах принимать решения о доработке (модернизации) систем защиты персональных данных, повторной оценки эффективности принятых мер по обеспечению безопасности или проведении дополнительных испытаний.

3.24. Требовать прекращения обработки персональных данных, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного режима обеспечения безопасности персональных данных или нарушения функционирования информационных систем.

3.25. Незамедлительно информировать заведующего Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» об имеющихся недостатках в функционировании систем защиты персональных данных, а также в случае возникновения инцидентов безопасности персональных данных в информационных системах.

3.26. Участвовать в проведении внутреннего расследования по фактам разглашения персональных данных, нарушения условий функционирования систем защиты персональных данных.

3.27. Организовывать проведение работ по защите персональных данных при выводе из эксплуатации информационной системы.

4. Права Ответственного

4.1. Ответственный имеет право:

4.1.1. Для проведения работ по обеспечению функционирования и работоспособности средств вычислительной техники, информационных технологий и программного обеспечения, используемых в информационных системах, а также технической поддержки и обслуживания баз данных, привлекать на договорной основе юридических лиц и индивидуальных предпринимателей.

4.1.2. Для проведения работ по созданию и внедрению систем защиты персональных данных информационных систем , а также оценки эффективности реализованных в рамках систем защиты персональных данных мер по обеспечению безопасности персональных данных при необходимости привлекать юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

4.1.3. Контролировать действия администраторов безопасности систем защиты персональных данных в соответствии с инструкциями указанных ответственных лиц.

4.2. Лицо, ответственное за обеспечение безопасности персональных данных в информационных системах, несет ответственность за:

4.2.1. Качество проводимых им работ по обеспечению защиты персональных данных в соответствии с задачами и обязанностями, предусмотренными в настоящей Инструкции.

4.2.2. Реализацию утвержденных в Муниципальном бюджетном дошкольном образовательном учреждении Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» организационно-распорядительных документов по защите персональных данных.

4.2.3. Разглашение информации ограниченного доступа, ставшей известной ему по роду работы.

Лист ознакомления
с Инструкцией ответственного за обеспечение безопасности персональных данных в информационных системах

№ п/п	**Ф.И.О.**	**Дата**	**Подпись**

УТВЕРЖДАЮ

Заведующий
Муниципальным бюджетным
дошкольным образовательным
учреждением Измалковского
муниципального района Липецкой
области «Детский сад «Сказка»
д. Денисово»
_____ О.В. Лошкарева
«09» сентября 2022 г.

Приложение №2 к Приказу № 95
от «09» сентября 2022 г.

ИНСТРУКЦИЯ
администратора безопасности системы защиты персональных данных информационной системы

1. Общие положения

1.1. Администратор безопасности системы защиты персональных данных информационной системы (далее – АБ) в Муниципальном бюджетном дошкольном образовательном учреждении Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» назначается приказом заведующим.

1.2. АБ в своей работе руководствуется положениями действующего законодательства о защите персональных данных, настоящей Инструкцией и иными локальными документами Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» по защите персональных данных.

1.3. Настоящая Инструкция определяет задачи, обязанности, права и ответственность АБ по вопросам обеспечения информационной безопасности при обработке персональных данных в информационной системе.

1.4. Методическое руководство работой АБ осуществляется Ответственным за обеспечение безопасности персональных данных в информационных системах (далее – ГИС).

2. Задачи АБ

2.1. Обеспечение работоспособности элементов ГИС, основных технических средств и систем (далее – ОТСС), локальной вычислительной сети.

2.2. Обеспечение бесперебойной работоспособности системы защиты информации ГИС и отдельных средств защиты информации.

2.3. Выявление инцидентов, которые могут привести к сбоям или нарушению функционирования ГИС или к возникновению новых угроз безопасности информации, и реагирование на них.

2.4. Восстановление системы защиты информации при сбоях.

2.5. Организация разграничения доступа пользователей к информационным ресурсам ГИС.

2.6. Оперативный контроль за работой пользователей.

2.7. Осуществление постоянного контроля за соблюдением требований по обеспечению информационной безопасности.

3. Обязанности АБ

3.1. Для реализации поставленных задач АБ обязан:

3.1.1. Вести поэкземплярный учет средств защиты информации, эксплуатационной и технической документации к ним, в том числе средств криптографической защиты информации, ключевых документов.

3.1.2. Вести учет машинных носителей персональных данных в соответствии организационной-распорядительной документацией Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово».

3.1.3. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания рабочих станций и отправке их в ремонт (контролировать стирание информации на машинных носителях).

3.1.4. Осуществлять резервное копирование персональных данных, содержащихся в ГИС с периодичностью, установленной в организационно-распорядительных документах Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово».

3.1.5. Информировать пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации ГИС и отдельных средств защиты информации, а также проводить обучение по работе с ними.

3.1.6. Осуществлять управление (администрирование) системой защиты информации ГИС, которое включает в себя:

- заведение и удаление учетных записей пользователей, управление полномочиями пользователей ГИС и поддержание правил разграничения доступа в информационной системе;
- генерацию, смену и восстановление паролей пользователей;
- управление средствами защиты информации в информационной системе, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации;
- установку обновлений программного обеспечения, включая программное обеспечение средств защиты информации;
- восстановление работоспособности средств защиты информации,
- централизованное управление системой защиты информации информационной системы (при необходимости);
- контроль синхронизации системного времени;
- ввод в базу данных системы защиты от НСД описания событий, подлежащих регистрации в системном журнале;
- анализ событий в информационной системе, связанных с защитой информации (далее – события безопасности), для выявления попыток несанкционированного доступа к защищаемым ресурсам;
- своевременное информирование Ответственного за обеспечение безопасности персональных данных в ГИС о несанкционированных действиях персонала и организацию расследования попыток НСД;
- своевременное архивирование журналов событий безопасности и надлежащий режим хранения данных архивов;
- настройку СЗИ способом, исключающим доступ к записям аудита и функциям управления механизмами регистрации (аудита) лицам, не имеющим полномочий на доступ;
- защиту персональных данных при взаимодействии пользователей с информационными сетями общего пользования.

3.1.7. Выявлять и реагировать на инциденты в системе защиты информации ГИС:

3.1.8. обнаруживать и идентифицировать инциденты, в том числе отказы в обслуживании, сбои (перезагрузок) в работе технических средств, программном обеспечения и средствах защиты информации, нарушении правил разграничения доступа, неправомерные действия по сбору информации, внедрению вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

- анализировать инциденты, в том числе определять источники и причины возникновения инцидентов, а также оценивать их последствия;
- планировать и принимать меры по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа,

неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– планировать и принимать меры по предотвращению повторного возникновения инцидентов.

3.1.9. С периодичностью, установленной в организационной-распорядительных документах Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово», обеспечивать внутренний контроль за соблюдением требований по обеспечению информационной безопасности, который включает в себя:

– контроль за событиями безопасности и действиями пользователей в информационной системе;

– контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;

– контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

– контроль состава технических средств, программного обеспечения и средств защиты информации;

– анализ и устранение недостатков в функционировании системы защиты информации информационной системы;

– документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности персональных данных, содержащихся в информационной системе.

3.1.10. Поддерживать конфигурацию ГИС и ее системы защиты в соответствии с эксплуатационной документацией.

3.1.11. Перед внесением изменений в конфигурацию ГИС и системы защиты информации ГИС проводить анализ потенциального воздействия планируемых изменений на обеспечение защиты персональных данных и согласовывать данные изменения с Ответственным за обеспечение безопасности персональных данных в ГИС.

3.1.12. Присутствовать при внесении изменений в конфигурацию аппаратно-программных средств защищенных рабочих станций и серверов.

3.1.13. Фиксировать все изменения в конфигурации информационной системы или функционирующей системе защиты информации в эксплуатационной документации.

3.1.14. Установку ПО осуществлять с учетом перечня ПО, разрешенного к установке. При необходимости установки дополнительного ПО, требуемого для выполнения должностных обязанностей пользователей или функционирования информационной системы, отсутствующего в данном перечне, инициировать принятие решения о включении ПО в перечень разрешенного к установке ПО совместно с Ответственным за обеспечение безопасности персональных данных в ГИС.

3.1.15. Обеспечивать защиту персональных данных при выводе из эксплуатации ГИС.

3.2. АБ запрещается:

3.2.1. Использовать служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ее модификации, копирования, уничтожения.

3.2.2. Использовать ставшие доступные в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий.

3.2.3. Использовать в своих и в чьих-либо личных интересах ресурсы информационной системы, предоставлять такую возможность другим.

3.2.4. Выключать СЗИ без санкции руководства.

3.2.5. Передавать третьим лицам сетевые адреса, имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки.

3.2.6. Производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы информационной системы, блокировке, потери информации и предупреждения пользователей.

3.2.7. Нарушать правила эксплуатации оборудования ГИС.

3.2.8. Корректировать, удалять, подменять журналы аудита.

4. Права и ответственность АБ

4.1. АБ имеет право:

4.1.1. Получать доступ к программным и аппаратным средствам ГИС, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах информационной системы и рабочих станций пользователей.

4.1.2. Требовать от пользователей ГИС выполнения инструкций по обеспечению безопасности.

4.1.3. Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов информационной системы.

4.1.4. Осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности.

4.1.5. Производить анализ защищенности информационной системы и попыток взлома системы защиты информационной системы путем применения специальных средств.

4.1.6. Вносить свои предложения по совершенствованию мер защиты в информационной системе.

4.2. АБ несет ответственность за:

4.2.1. Программно-технические и криптографические средства защиты информации, средства вычислительной техники, информационно-вычислительные комплексы, сети и автоматизированные системы обработки информации.

4.2.2. Качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

Лист ознакомления
с Инструкцией администратора безопасности системы защиты персональных данных
информационной системы

№ п/п	**Ф.И.О.**	**Дата**	**Подпись**

УТВЕРЖДАЮ

Заведующий
Муниципальным бюджетным
дошкольным образовательным
учреждением Измалковского
муниципального района Липецкой
области «Детский сад «Сказка»
д. Денисово»
_____ О.В. Лошкарева
«09» сентября 2022 г.

Приложение №3 к Приказу № 95
от «09» сентября 2022 г.

ИНСТРУКЦИЯ
пользователя информационной системы

1. Общие положения

1.1. Настоящая инструкция определяет обязанности, права и ответственность пользователей, допущенных к обработке персональных данных в информационной системе (далее – ГИС) Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово».

1.2. Пользователями ГИС являются сотрудники Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово», допущенные к обработке персональных данных в ГИС согласно утвержденным Перечням сотрудников Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово», доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими трудовых обязанностей.

1.3. Перед началом работ пользователь должен ознакомиться с содержанием:

- Эксплуатационной документации пользователя на установленные в ГИС средства защиты информации;
- Организационно-распорядительных документов по вопросам обеспечения защиты информации в части его касающейся.

1.4. Оперативный контроль за действиями пользователей при работе в ГИС осуществляет Администратор безопасности, который имеет право приостановить обработку персональных данных в случае выявления нарушений.

2. Обязанности пользователя

Пользователь обязан:

- выполнять требования настоящей инструкции, требования организационно-распорядительных документов по разграничению доступа к информационным ресурсам, а также требования организационно-технических документов по безопасности персональных данных;
- применять меры, препятствующие компрометации идентификаторов и паролей;
- использовать для обработки персональных данных только штатные программные и технические средства ГИС. Для хранения персональных данных использовать только специально выделенные Администратором безопасности каталоги на жестком магнитном диске, либо соответствующим образом учтенные внешние носители информации.
- знать штатные режимы работы программного обеспечения, используемого при обработке информации, в т. ч. средств защиты информации;

- соблюдать правила работы с АРМ, со средствами защиты информации установленными в ГИС, согласно заводскому руководству пользователей по эксплуатации этих средств;

- при возникновении подозрения на наличие в ГИС вредоносного программного обеспечения (вируса) провести внеочередную проверку АРМ на наличие вирусов с использованием штатных антивирусных программ;

- при работе с внешними носителями информации перед началом работы проверить их на наличие вирусов с использованием штатных антивирусных программ, установленных в ГИС;

- в случае обнаружения вирусов на стационарном или внешнем носителе информации немедленно сообщить о данном факте Администратору безопасности;

- принимать меры, препятствующие несанкционированному доступу к персональным данным данных, отображаемым на экране монитора, распечатках принтера и т.д. В случае оставления рабочего места на время перерыва, произвести блокировку или выключение АРМ.

- принимать меры по защите внешних носителей информации от несанкционированного доступа. Хранение внешних носителей информации осуществляется в недоступном для посторонних лиц месте (в сейфе, в ящике стола под замком);

- использовать сети общего доступа и (или) международного обмена (Интернет) только для исполнения служебных обязанностей. При передаче через Интернет защищаемой информации использовать соответствующие средства защиты информации (межсетевые экраны, средства шифрования, средства обнаружения вторжения);

- обо всех выявленных фактах несанкционированного доступа к информации, нарушениях, связанных с информационной безопасностью незамедлительно сообщать Администратору безопасности.

- своевременно информировать лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе.

3. Права пользователя

3.1. Пользователь имеет право:

- использовать штатные программно-аппаратные средства ГИС для решения профессиональных задач в соответствии с установленными Администратором безопасности правами доступа;

- обращаться к Администратору безопасности с просьбой об оказании технической и методической помощи в работе по обеспечению безопасности персональных данных;

- обращаться к Администратору безопасности с требованием о прекращении обработки защищаемой информации, в случаях нарушения установленной технологии обработки информации, выявления нарушений информационной безопасности или выхода из строя средств защиты информации.

3.2. Пользователю запрещается:

- осуществлять попытки несанкционированного доступа к ресурсам ГИС в нарушение установленных правил разграничения доступа;

- подменять функции Администратора безопасности по изменению настроек СрЗИ, изменению времени работы пользователей и их полномочий доступа к ресурсам ГИС;

- сообщать (или передавать) посторонним лицам личные идентификаторы и пароли доступа к ресурсам ГИС, оставлять аппаратные идентификаторы без присмотра;

- фиксировать на любых носителях персональный пароль (распечатывать на бумаге, писать на клавиатуре, мониторе и прочих предметах);

- вносить изменения в аппаратную, программную и логическую конфигурацию ГИС;

- осуществлять вскрытие опечатывающих элементов корпусов средств вычислительной техники;

- подключать к АРМ нештатные блоки и устройства, использовать неучтенные внешние носители информации (оптические диски, гибкие магнитные диски, флэш-накопители, мобильные устройства);

- изменять места расположения основных технических средств и систем (далее – ОТСС) ГИС без согласования с Администратором безопасности.

- использовать для хранения персональных данных каталоги, не предназначенные для этого Администратором безопасности;

- использовать учтенные служебные внешние носители информации для хранения информации, не имеющей отношения к выполняемым работам;

- использовать внешний носитель информации или АРМ при обнаружении на них вируса до устранения данной угрозы Администратором безопасности;

- устанавливать на АРМ программное обеспечение, выполнять действия, не связанные с исполнением служебных обязанностей;

- при работе в сетях общего доступа и (или) международного обмена (Интернет) осуществлять передачу защищаемой информации при отключенных средствах защиты информации;

- нецелевое использование сетей общего доступа и (или) международного обмена (Интернет);

- изменять состав, расположение и способы подключения основных технических средств ГИС без согласования с Администратором безопасности;

- оставлять учтенные внешние носители информации и разработанные документы бесконтрольно, оставлять во время перерыва рабочее место не выполнив блокировку АРМ;

- проводить обработку персональных данных в ГИС при неработоспособных или отключенных средствах защиты информации, либо выявленных нарушениях информационной безопасности.

- при обработке персональных данных произносить их вслух (по телефону, печатать под диктовку и т.п.) даже при отсутствии в помещении посторонних лиц.

4. Ответственность пользователя

Пользователь несет персональную ответственность за:

- за соблюдение правил эксплуатации ГИС, требований по безопасности информации, сохранность защищаемой информации, документов и электронных носителей информации, персональных идентификаторов, с которыми он работает;

- правильность и полноту выполнения целей, задач, функций, прав и обязанностей, возложенных на него;

- выполнение указаний Администратора безопасности, касающихся работы в ГИС и защиты информации.

Лист ознакомления
с Инструкцией пользователя информационной системы

№ п/п	**Ф.И.О.**	**Дата**	**Подпись**

УТВЕРЖДАЮ

Заведующий
Муниципальным бюджетным
дошкольным образовательным
учреждением Измалковского
муниципального района Липецкой
области «Детский сад «Сказка»
д. Денисово»
_____ О.В. Лошкарева
«09» сентября 2022 г.

Приложение №4 к Приказу № 95
от «09» сентября 2022 г.

ИНСТРУКЦИЯ
по организации резервного копирования и восстановления персональных данных в информационной системе

1. Общие положения

1.1. Настоящая Инструкция устанавливает основные требования к организации резервного копирования и восстановления персональных данных, содержащихся в государственной информационной системе (далее – ГИС) Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово».

1.2. Ответственность за организацию резервного копирования и восстановления персональных данных в ГИС возлагается на Администратора безопасности.

1.3. Резервное копирование осуществляется на носители, определённые в настоящей инструкции.

1.4. Периодичность резервного копирования проводится в сроки, определённые настоящей Инструкцией.

1.5. Ответственность за надлежащее хранение резервных носителей персональных данных, возлагается на Администратора безопасности.

1.6. Учет резервных носителей персональных данных осуществляется в соответствии с Инструкцией по организации учета, использования и уничтожения машинных носителей, предназначенных для обработки и хранения персональных данных в информационной системе.

2. Информация, подлежащая резервному копированию

2.1. Информация, обрабатываемая в Муниципальном бюджетном дошкольном образовательном учреждении Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» может быть разделена на следующие типы:

- системное программное обеспечение;
- прикладное программное обеспечение общего назначения;
- специализированное программное обеспечение;
- открытая информация;
- информация ограниченного доступа (персональные данные).

2.2. Системное программное обеспечение поставляется производителем программного обеспечения и не требует организации резервного копирования. Если это программное обеспечение поставляется на других носителях, то возможность его копирования определяется лицензионным соглашением с производителем.

2.3. Прикладное программное обеспечение общего назначения также поставляется производителем данного программного обеспечения. Возможности его копирования (в том

числе для резервного хранения) определяются условиями лицензионного соглашения. Как правило, современное программное обеспечение поставляется на CD\DVD-ROM и не требует резервного копирования.

2.4. Носители со специализированным программным обеспечением должны храниться в соответствии с Инструкцией по организации учета использования и уничтожения машинных носителей, предназначенных для обработки и хранения персональных данных в информационной системе. Лица, имеющие доступ к носителям и отвечающие за их сохранность, не должны допускать несанкционированного копирования носителей со специализированным программным обеспечением.

2.5. Открытая информация - это информация, доступная всем лицам, а также информация, предназначенная для опубликования в открытой печати. Открытая информация подлежит обязательному резервному копированию с периодичностью, определяемой настоящей инструкцией.

2.6. Информация ограниченного доступа (персональные данные) подлежит обязательному резервному копированию. Доступ к информации и её резервной копии должен быть ограничен в соответствие с Положением о разрешительной системе доступа к информационным ресурсам информационной системы. Резервное копирование персональных данных должно производиться только на носители, предназначенные для хранения персональных данных, в соответствии с Инструкцией по организации учета, использования и уничтожения машинных носителей, предназначенных для обработки и хранения персональных данных в информационной системе.

3. Аппаратное обеспечение резервного копирования и восстановления информации

3.1. Для резервного копирования и восстановления информации Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» оборудовано соответствующими техническими средствами.

3.2. Машинные носители, предназначенные для длительного хранения информации, должны периодически проверяться на их пригодность и отсутствие сбойных секторов. При появлении сбойных секторов на машинных носителях информация с этих носителей должна переносится на исправные. Если на неисправных носителях содержалась персональных данных, то они должны уничтожаться в соответствии с Инструкцией по организации учета, использования и уничтожения машинных носителей, предназначенных для обработки и хранения персональных данных в информационной системе.

4. Периодичность резервного копирования

4.1. Резервное копирование специализированного программного обеспечения производиться при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

4.2. Информация (открытая и ограниченного доступа), содержащаяся в постоянно изменяемых базах данных информационных систем, должна сохраняться в соответствии со следующим графиком:

– ежедневно должно проводиться копирование изменённой и дополненной информации. Носители с ежедневной информацией должны храниться в течение недели.

– еженедельно должно проводиться резервное копирование всей базы данных. Носители с еженедельными копиями хранятся в течение месяца.

– ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

5. Восстановление информации

5.1. Восстановление информации происходит в случае её исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок персонала и аппаратных сбоев.

5.2. Восстановление системного программного обеспечения и прикладного программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

5.3. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

5.4. Восстановление открытой информации и информации ограниченного доступа производится с резервных носителей. При этом необходимо использовать последнюю копию информации.

При частичном нарушении или исчезновении записей баз данных восстановление производится с последней не нарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

Лист ознакомления
с Инструкцией по организации резервного копирования и восстановления
персональных данных в информационной системе

№ п/п	**Ф.И.О.**	**Дата**	**Подпись**

УТВЕРЖДАЮ

Заведующий
Муниципальным бюджетным
дошкольным образовательным
учреждением Измалковского
муниципального района Липецкой
области «Детский сад «Сказка»
д. Денисово»
_____ О.В. Лошкарева
«09» сентября 2022 г.

Приложение №5 к Приказу № 95
от «09» сентября 2022 г.

ИНСТРУКЦИЯ
по организации учета, использования и уничтожения машинных носителей, предназначенных для обработки и хранения персональных данных в информационной системе

Общие положения

1.1. Настоящая Инструкция устанавливает основные требования к организации учета и использования машинных носителей, предназначенных для обработки и хранения персональных данных информационной системе (далее – ГИС) Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово».

1.2. Ответственность за организацию учета и использования машинных носителей, предназначенных для обработки и хранения персональных данных, возлагается на Администратора безопасности.

1.3. Все машинные носители данных, используемые при работе со средствами вычислительной техники (СВТ) для обработки и хранения персональных данных, должны обязательно регистрироваться и учитываться. Допускается автоматизированный учет машинных носителей персональных данных.

1.4. Проверка наличия машинных носителей персональных данных, проводится в сроки, установленные настоящей Инструкцией.

2. Учет машинных носителей персональных данных

2.1. К машинным носителям персональных данных относятся:

– съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

– портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты и иные аналогичные по функциональности устройства);

– машинные носители, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

2.2. Персональную ответственность за сохранность полученных машинных носителей данных и предотвращение несанкционированного доступа к записанной на них информации несет работник, получивший эти носители.

2.3. При обработке персональных данных должен соблюдаться следующий общий порядок учета, хранения и уничтожения машинных носителей данных.

2.4. Поэкземплярный учет машинных носителей данных из п. 2.1., предназначенных для записи персональных данных производится в Журнале учета и выдачи машинных носителей персональных данных с использованием заводских номеров.

2.5. Хранение машинных носителей должно осуществляться в условиях, исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.

2.6. Право физического доступа к машинным носителям и право на перемещение машинных носителей за пределы контролируемой зоны работник получает в соответствии с Положением о разрешительной системе доступа к информационным ресурсам информационных систем и Матрицей доступа.

2.7. Машинные носители данных выдаются операторам или другим лицам, участвующим в обработке персональных данных, для работы под расписку в Журнале учета и выдачи машинных носителей персональных данных. По завершению работы машинные носители данных сдаются Администратору безопасности.

2.8. Не съемные жесткие магнитные диски закрепляются за работником, ответственным за СВТ, в котором они установлены.

2.9. Машинные носители данных после стирания с них персональных данных с учета не снимают, а хранятся наравне с машинными носителями персональных данных.

2.10. В последующем эти носители используются для записи персональных данных. Если носители не пригодны для дальнейшего использования, они подлежат уничтожению.

2.11. В случае повреждения машинных носителей персональных данных работник, в пользовании которого они находятся, обязан сообщить о случившемся своему непосредственному руководителю.

2.12. О фактах утраты машинных носителей незамедлительно докладывается Администратору безопасности и проводится служебное расследование.

2.13. Копирование персональных данных с целью передачи работнику, не входящему в Перечень сотрудников Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово», доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими трудовых обязанностей, осуществляется только с разрешения заведующего Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово».

2.14. Передача персональных данных третьим лицам в рамках осуществления деятельности, предусмотренной действующим законодательством Российской Федерации (включая передачу отчетности в ПФР, ФНС, ФСС), осуществляется уполномоченными работниками во исполнение своих трудовых обязанностей. Передача данных осуществляется в срок и в форме, предусмотренной законодательством Российской Федерации, и не требует согласования с руководством.

2.15. Передача персональных данных иным третьим лицам (по запросу) осуществляется исключительно Ответственным за организацию обработки персональных данных с письменного разрешения Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово», при этом делается соответствующая запись в Журнале учета передачи персональных данных по запросам третьих лиц.

2.16. Проверка наличия и условий хранения машинных носителей персональных данных проводится Ответственным за обеспечение безопасности персональных данных в информационных системах не реже, чем 1 раз в полгода.

3. Порядок уничтожения машинных носителей, предназначенных для обработки и хранения персональных данных

3.1. Уничтожение (стирание) данных и остаточной информации с машинных носителей персональных данных производится при необходимости передачи машинного носителя другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

3.2. Уничтожение машинных носителей персональных данных, пришедших в негодность или утративших практическую ценность, производится путем их физического

разрушения. Перед уничтожением носителя информация с него должна быть стерта (уничтожена), если это позволяют физические принципы работы носителя.

3.3. Списание машинных носителей данных производится комиссией, назначаемой заведующим Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово».

3.4. Акты об уничтожении машинных носителей, содержащих персональные данные, подписываются председателем комиссии, ее членами и утверждаются заведующим Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово».

3.5. При уничтожении машинные носители данных снимаются с материального учета.

Лист ознакомления
с Инструкцией по организации учета, использования и уничтожения машинных носителей, предназначенных для обработки и хранения персональных данных в информационной системе

№ п/п	**Ф.И.О.**	**Дата**	**Подпись**

УТВЕРЖДАЮ

Заведующий
Муниципальным бюджетным
дошкольным образовательным
учреждением Измалковского
муниципального района Липецкой
области «Детский сад «Сказка»
д. Денисово»
_____ О.В. Лошкарева
«09» сентября 2022 г.

Приложение №6 к Приказу № 95
от «09» сентября 2022 г.

ИНСТРУКЦИЯ
по организации парольной защиты в информационной системе

Общие положения

1.1. Ответственность за своевременность смены пароля несут пользователи информационной системы Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово».

1.2. Ответственность за сохранность списка паролей несет Администратор безопасности.

1.3. Список паролей пользователей информационной системы ведется Администратором безопасности, в единственном экземпляре карандашом.

1.4. Запись о выдаче или смене пароля пользователя заносится в Журнал учета выдачи паролей.

2. Правила формирования пароля

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в составе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (“ ~ ! @ # $ % ^ & * ( ) - + _ = \ | / ? ,);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;
- личный пароль пользователь не имеет права сообщать никому;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе.

3. Порядок смены паролей

3.1 Полная плановая смена паролей пользователей должна осуществляется не реже одного раза в 90 дней.

3.2 Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую должность и т.п.) должна производиться Администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

3.3 Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) Администратора безопасности и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой информационной системы.

3.4 В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с п.3.2 или п.3.3 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

3.5 Факт смены пароля Администратор безопасности и работник Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово», меняющий пароль, подтверждают росписями в Журнале учета выдачи паролей, хранящемся в пакете вместе со списками паролей.

3.6 По заполнении Журнал учета выдачи паролей хранится у Администратора безопасности в Муниципальном бюджетном дошкольном образовательном учреждении Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» до конца текущего года, затем уничтожается.

4. Порядок доступа к списку паролей в экстренных случаях

4.1 В экстренных случаях, когда доступ к конкретному паролю необходимо осуществить в отсутствии его владельца, непосредственный руководитель работника, чей пароль необходимо выяснить (далее – непосредственный руководитель), обращается с запросом в письменной форме к заведующему Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» с просьбой разрешить доступ к паролю данного своего подчиненного.

4.2 Администратор безопасности, получив письменное распоряжение заведующего Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» (в виде резолюции на запросе), вскрывает пакет со списком паролей, выписывает необходимый пароль на бумажный носитель и передает его непосредственному руководителю.

4.3 Факт вскрытия пакета непосредственный руководитель и Администратор безопасности подтверждают росписями в Журнале учета выдачи паролей.

4.4 Непосредственный руководитель информирует подчиненного о факте использования его пароля во время его отсутствия.

Лист ознакомления
с Инструкцией по организации парольной защиты в информационной системе
персональных данных

№ п/п	**Ф.И.О.**	**Дата**	**Подпись**

УТВЕРЖДАЮ

Заведующий
Муниципальным бюджетным
дошкольным образовательным
учреждением Измалковского
муниципального района Липецкой
области «Детский сад «Сказка»
д. Денисово»
_____ О.В. Лошкарева
«09» сентября 2022 г.

Приложение №7 к Приказу № 95
от «09» сентября 2022 г.

ИНСТРУКЦИЯ
по применению средств антивирусной защиты информации в информационной системе

1. Основные положения

1.1. Настоящая Инструкция разработана в целях осуществления антивирусной защиты информации, содержащейся и обрабатываемой на рабочих станциях информационных систем Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» и ЛВС, от несанкционированного копирования, модификации и разрушения, а также нарушения работы используемого программного обеспечения при воздействии вирусов и других вредоносных программ посредством комплекса организационно-технических мероприятий по обеспечению информационной безопасности.

1.2. Настоящая Инструкция определяет порядок применения средств антивирусной защиты, порядок обновления баз данных средств антивирусной защиты информации, задачи, обязанности и права Администратора безопасности и пользователей средств антивирусной защиты информации, порядок их действий при обнаружении программных вирусов, а также ответственность за невыполнение требований настоящей Инструкции.

1.3. Требования настоящей Инструкции обязательны для выполнения пользователями информационной системы и Администратором безопасности, а также иными лицами, использующими средства вычислительной техники.

1.4. Практическое решение задач, связанных с организацией антивирусной защиты информации и применением средств антивирусной защиты, осуществляется Администратором безопасности.

2. Порядок применения средств антивирусной защиты информации

2.1. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово», обрабатывающих персональные данные.

2.2. Порядок применения средств антивирусной защиты информации устанавливается с учетом соблюдения следующих требований:

- обязательный входной контроль за отсутствием программных вирусов во всех поступающих на объект информатизации электронных носителях информации, информационных массивах, программных средствах общего и специального назначения;
- обязательная проверка всех электронных писем на предмет отсутствия программных вирусов;
- периодическая проверка на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка съемных

носителей информации перед началом работы с ними;

– внеплановая проверка жестких магнитных дисков и съемных носителей информации в случае подозрения на наличие программных вирусов;

– восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

2.3. Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

2.4. Копирование любой информации, переносимой с помощью любых съемных носителей информации, должно производиться только после проведения процедуры полного антивирусного контроля съемного носителя.

2.5. Антивирусная профилактика является необходимым элементом защиты информационных ресурсов от их модификации и уничтожения. Антивирусная профилактика состояния средств антивирусной защиты информации на серверах и рабочих станциях должна, как правило, проводиться по согласованию с Администратором безопасности.

3. Порядок обновления баз данных средств антивирусной защиты информации

3.1. Своевременное обновление баз данных средств антивирусной защиты информации является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.

3.2. Обновление баз данных средств антивирусной защиты информации на рабочих станциях и серверах в ЛВС осуществляется в автоматическом режиме.

3.3. На рабочем месте Администратора безопасности могут быть установлены средства, позволяющие через ЛВС управлять компонентами системы антивирусной защиты, установленными на рабочих станциях и серверах, а также проводить обновления баз средств антивирусной защиты информации. В случае если рабочая станция пользователя не подключена к ЛВС, обновление средств антивирусной защиты информации производится пользователем через съемные носители информации. Периодичность обновления определяется программными требованиями средств антивирусной защиты информации или устанавливается Администратором безопасности.

4. Обязанности и права Администратора безопасности

4.1. Администратор безопасности обязан обеспечивать соблюдение политики антивирусной защиты информации и выявление фактов заражения программными вирусами.

4.2. К основным задачам Администратора безопасности относятся организация процесса установки и обновления средств антивирусной защиты информации на рабочих станциях пользователей и обеспечение технического сопровождения действий пользователей в случаях обнаружения программных вирусов, а также осуществление контроля за состоянием системы антивирусной защиты информации.

4.3. Администратор безопасности несет ответственность:

– за своевременную установку средств антивирусной защиты информации;

– за эксплуатацию системы антивирусной защиты информации;

– за своевременное обновление лицензий на средства антивирусной защиты информации;

– за своевременное обновление баз данных средств антивирусной защиты информации.

4.4. Администратор безопасности имеет право:

– осуществлять контроль состояния средств антивирусной защиты;

– проводить служебные проверки по фактам заражения программными вирусами автоматизированных систем обработки информации и средств вычислительной техники;

– оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты информации.

5. Обязанности пользователей средств антивирусной защиты информации

5.1. Пользователь обязан изучить настоящую Инструкцию и ознакомиться с необходимостью несения ответственности за выполнение ее требований под роспись.

5.2. Пользователям запрещается:

– отключать средства антивирусной защиты информации во время работы;

– без разрешения Администратора безопасности копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

5.3. В случае появления подозрений на наличие программных вирусов в ЛВС пользователи должны немедленно проинформировать об этом Администратора безопасности. В случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств антивирусной защиты, пользователь обязан незамедлительно сообщить об этом администратору безопасности.

6. Порядок действий пользователей и Администратора безопасности при обнаружении вирусов

6.1. В случае обнаружения программных вирусов при входном контроле отчуждаемых носителей информации, файлов или почтовых сообщений пользователь должен:

– приостановить процесс приема-передачи информации;

– сообщить Администратору безопасности о факте обнаружения программного вируса;

– принять по согласованию с Администратором безопасности меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.

6.2. При обнаружении программных вирусов в процессе обработки информации пользователь обязан:

– немедленно приостановить все работы;

– сообщить Администратору безопасности о факте обнаружения программных вирусов;

– принять по согласованию с Администратором безопасности меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.

6.3. При невозможности ликвидации последствий заражения программными вирусами Администратору безопасности необходимо:

– сообщить юридическому лицу или индивидуальному предпринимателю, осуществляющему техническую поддержку эксплуатации средств антивирусной защиты информации;

– заархивировать зараженные файлы с внедренными программными вирусами и направить в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;

– осуществить полную переустановку программного обеспечения на зараженном компьютере.

6.4. При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на рабочей станции данного пользователя незамедлительно блокируется по решению Администратора безопасности.

6.5. Все факты модификации и разрушения данных на серверах или рабочих станциях, заражение их вирусами, а также обнаружение других вредоносных программ классифицируются как значимые нарушения информационной безопасности и должны анализироваться посредством проведения служебного расследования.

7. Порядок информирования о вирусной активности

7.1. Своевременное информирование о вирусной активности является составной частью системы антивирусной защиты информации.

7.2. Информирование (распространение предупреждений) о вирусной активности осуществляется централизованно через электронную почту посредством автоматической рассылки или иным способом по усмотрению Администратора безопасности.

8. Порядок оснащения средствами антивирусной защиты информации

8.1. Оснащение средствами антивирусной защиты информации является видом

материального обеспечения и осуществляется централизованно.

8.2. За несанкционированное распространение средств антивирусной защиты информации виновные несут ответственность в соответствии с законодательством Российской Федерации.

9. Ответственность за выполнение требований Инструкции

9.1. За нарушение настоящей Инструкции Администратор безопасности и пользователи несут ответственность, установленную действующим законодательством Российской Федерации и нормативными правовыми актами.

9.2. Руководитель отдела несет ответственность за выполнение мероприятий по антивирусной защите информации на средствах вычислительной техники, эксплуатируемых подчиненными лицами, и за ознакомление их (под роспись) с настоящей Инструкцией.

9.3. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации на своих рабочих местах, в том числе за своевременное обновление антивирусных баз средств антивирусной защиты информации и получение новых лицензионных ключей, несут пользователи, за которыми закреплены средства вычислительной техники.

9.4. В случае нарушения требований настоящей Инструкции, связанных с применением пользователем средств антивирусной защиты информации, пользователь несет персональную ответственность, установленную действующим законодательством Российской Федерации и нормативно правовыми актами.

9.5. Ответственность за выполнение требований настоящей Инструкции несет Администратор безопасности.

Лист ознакомления
с Инструкцией по применению средств антивирусной защиты информации в информационной системе

№ п/п	**Ф.И.О.**	**Дата**	**Подпись**

УТВЕРЖДАЮ

Заведующий
Муниципальным бюджетным
дошкольным образовательным
учреждением Измалковского
муниципального района Липецкой
области «Детский сад «Сказка»
д. Денисово»
_____ О.В. Лошкарева
«09» сентября 2022 г.

Приложение №8 к Приказу № 95
от «09» сентября 2022 г.

ИНСТРУКЦИЯ
по обеспечению защиты персональных данных при выводе из эксплуатации информационной системы

1. Общие положения

1.1. Настоящая Инструкция устанавливает основные требования защиты персональных данных при выводе из эксплуатации информационной системы (далее – ГИС) Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово» или после принятия решения об окончании обработки персональных данных.

1.2. Обязанности по выполнению требований настоящей Инструкции возлагаются на Администратора безопасности.

1.3. Ответственность за организацию защиты персональных данных при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки персональных данных возлагается на Ответственного за обеспечение безопасности персональных данных в информационных системах.

2. Порядок организации защиты персональных данных при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки персональных данных

2.1. Обеспечение защиты персональных данных при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки персональных данных осуществляется в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите персональных данных.

2.2. Методы защиты информации включают:

- архивирование информации, содержащейся в информационной системе;
- уничтожение (стирание) данных и остаточной информации с машинных носителей персональных данных и (или) уничтожение машинных носителей персональных данных.

2.3. Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности Муниципального бюджетного дошкольного образовательного учреждения Измалковского муниципального района Липецкой области «Детский сад «Сказка» д. Денисово».

2.4. Уничтожение (стирание) данных и остаточной информации с машинных носителей персональных данных производится при необходимости передачи машинного носителя другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

2.5. При выводе из эксплуатации машинных носителей персональных данных, на которых осуществлялись хранение и обработка персональных данных, осуществляется физическое уничтожение этих машинных носителей.

2.6. Детализация проводимых работ по архивированию и уничтожению информации приведена в Инструкции по организации учета использования и уничтожения машинных носителей, предназначенных для обработки и хранения персональных данных в информационной системе.

2.7. Обо всех изменениях в части обработки и защиты персональных данных Администратор безопасности обязан уведомлять Ответственного за организацию обработки персональных данных и Ответственного за обеспечение безопасности персональных данных в информационных системах.

Лист ознакомления
с Инструкцией по обеспечению защиты персональных данных при выводе из эксплуатации информационной системы

№ п/п	**Ф.И.О.**	**Дата**	**Подпись**