УТВЕРЖДЕНО:
Заведующий МБДОУ
«Октябрьский ДС»
_____М.В.Каргина
приказ № 128 от 30.12.2025г.

Муниципальное бюджетное дошкольное образовательное учреждение
«Октябрьский детский сад № 19 «Дюймовочка»
(МБДОУ «Октябрьский ДС»)

Положение
об информационной безопасности муниципального бюджетного дошкольного образовательного учреждения «Октябрьский детский сад № 19 «Дюймовочка»
(МБДОУ «Октябрьский ДС»)

Х. Белогорский
2025 г.

1. Общие положения

1.1. Настоящее Положение об информационной безопасности (далее — Положение) муниципального бюджетного дошкольного образовательного учреждения «Октябрьский детский сад № 19 «Дюймовочка» (МБДОУ «Октябрьский ДС») (далее — ДОУ) разработано в соответствии с:

Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

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

1.2. Положение определяет задачи, функции, обязанности, ответственность и права лиц, ответственных за информационную безопасность в ДОУ.

1.3. Лица, ответственные за информационную безопасность, назначаются приказом заведующего ДОУ.

1.4. Лица, ответственные за информационную безопасность, подчиняются непосредственно заведующему ДОУ.

1.5. В своей работе лица, ответственные за информационную безопасность, руководствуются настоящим Положением, локальными актами ДОУ и актуальными нормативными документами в сфере информационной безопасности.

1.6. Лица, ответственные за информационную безопасность, обеспечивают защиту информации, обрабатываемой, передаваемой и хранимой с использованием информационных средств в ДОУ, в пределах своих функциональных обязанностей.

2. Основные задачи и функции ответственных за информационную безопасность

2.1. Основными задачами ответственных за информационную безопасность являются:

2.1.1. Организация эксплуатации технических и программных средств защиты информации с учётом современных угроз.

2.1.2. Текущий контроль работы средств и системы защиты информации, включая мониторинг инцидентов информационной безопасности.

2.1.3. Организация и контроль резервного копирования информации на серверах локальной вычислительной сети (ЛВС) с соблюдением требований к срокам хранения и восстановлению данных.

2.2. Ответственные за информационную безопасность выполняют следующие основные функции:

2.2.1. Разработка и актуализация инструкций по информационной безопасности, в т.ч.:

инструкции по организации антивирусной защиты;

инструкции по безопасной работе в сети Интернет;

инструкции по работе с персональными данными.

2.2.2. Обучение персонала и пользователей персональных компьютеров (далее — ПК) правилам безопасной обработки информации и правилам работы со средствами защиты информации, проведение регулярных инструктажей.

2.2.3. Организация антивирусного контроля съёмных носителей информации и файлов электронной почты, поступающих в ДОУ.

2.2.4. Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации.

2.2.5. Контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём.

2.2.6. Контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК, включая документирование всех изменений.

2.2.7. Контроль использования сети Интернет сотрудниками и пользователями ДОУ, в т. ч. соблюдение правил безопасного доступа.

2.2.8. Мониторинг и предотвращение утечек информации, в т. ч. персональных данных.

3. Обязанности ответственных за информационную безопасность

3.1. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах, возложенных на них обязанностей. Немедленно докладывать заведующему ДОУ о выявленных нарушениях и несанкционированных действиях пользователей и сотрудников, а также принимать необходимые меры по устранению нарушений.

3.2. Совместно с IT-специалистами (при наличии) или привлечёнными подрядчиками принимать меры по восстановлению работоспособности средств и систем защиты информации.

3.3. Проводить инструктаж сотрудников и пользователей ПК по правилам работы с используемыми средствами и системами защиты информации не реже одного раза в год и при изменении нормативных требований.

3.4. Создавать и удалять учётные записи пользователей в соответствии с утверждёнными правилами доступа.

3.5. Администрировать работу сервера ЛВС: размещать и классифицировать информацию на сервере ЛВС с учётом требований к защите данных.

3.6. Устанавливать по согласованию с заведующим ДОУ критерии доступа пользователей на сервер ЛВС, включая разграничение прав доступа.

3.7. Формировать и предоставлять пароли для новых пользователей, администрировать права пользователей, включая периодическую смену паролей и блокировку неактивных учётных записей.

3.8. Отслеживать работу антивирусных программ, проводить полную проверку компьютеров на наличие вирусов не реже одного раза в неделю, а также по мере необходимости при выявлении подозрительной активности.

3.9. Выполнять регулярное резервное копирование данных на сервере (не

реже одного раза в сутки), при необходимости восстанавливать потерянные или повреждённые данные.

3.10. Ежемесячно подавать заведующему ДОУ отчёт по использованию сети Интернет, включая статистику по трафику и выявленным инцидентам.

3.11. Вести учёт пользователей «точки доступа к Интернету». В случае необходимости ограничивать время работы пользователя в Интернете и объём скачиваемой информации в соответствии с утверждённым регламентом.

3.12. Незамедлительно сообщать заведующему ДОУ о выявлении случаев несанкционированного доступа в Интернет или иных инцидентов информационной безопасности.

3.13. Обеспечивать соответствие информационных систем ДОУ актуальным требованиям законодательства в области защиты персональных данных и информационной безопасности.

4. Права ответственных лиц за информационную безопасность

4.1. Требовать от сотрудников и пользователей компьютерной техники безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения, персональные данные и иную конфиденциальную информацию.

4.2. Готовить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов, в т. ч. по внедрению новых технологий защиты.

4.3. Запрашивать у сотрудников ДОУ необходимую информацию и документы, связанные с обеспечением информационной безопасности.

4.4. Приостанавливать доступ к информационным ресурсам в случае выявления нарушений требований информационной безопасности до устранения причин.

5. Ответственность лиц за информационную безопасность

5.1. На ответственных лиц за информационную безопасность возлагается персональная ответственность за качество проводимых ими работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определёнными настоящим Положением, и требованиями законодательства РФ.

5.2. Лица, ответственные за информационную безопасность, несут ответственность за:

несоблюдение требований законодательства в области информационной безопасности и защиты персональных данных;

ненадлежащее исполнение или неисполнение своих должностных обязанностей;

несвоевременное информирование руководства о выявленных инцидентах информационной безопасности;

утрату или несанкционированное распространение защищаемой информации.