

Муниципальное бюджетное дошкольное образовательное учреждение детский сад
комбинированного вида №76 город Ставрополь

Принято
Педагогическим советом
МБДОУ д/с №76
Протокол №1 от 30 августа 2022г.

Утверждаю:
Заведующий МБДОУ д/с №76
_____ С. Н.Резникова

Положение
об ответственном лице за обеспечение информационной безопасности во
время доступа к сети Интернет и внедрение системы контентной фильтрации
в образовательном учреждении.

1. Общие положения

1.1. Настоящее Положение об ответственном лице за обеспечение информационной безопасности во время доступа к сети Интернет и внедрение системы контентной фильтрации в образовательном учреждении (далее - Положение) Муниципального бюджетного дошкольного образовательного учреждения детского сада комбинированного вида № 76 города Ставрополя (далее - Учреждения) разработано в соответствии с:

- Федеральным законом от 27.07.2006 № Н9-ФЗ «Об информации, информационных технологиях и о защите информации»,
- Приказа ФСТЭК России от 02.2013 N 17 (ред. от 28.05.2019) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Зарегистрировано в Минюсте России 31.05.2013 № 28608),
- Федерального закона от 29.12.2010 N 436-ФЗ (ред. От 29.07.2018) «О защите детей от информации, причиняющей вред их здоровью и развитию», Распоряжения Правительства РФ от 02.12.2015 № 2471-р «Об утверждении Концепции информационной безопасности детей»
- Приказа Минкомсвязи России от 27.02.2018 N 88 «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018 - 2020 годы»
- Письма Минобрнауки России от 14.05.2018 N 08-1184 «О направлении

информации» (вместе с «Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети «Интернет»)

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (редакция от 28.06.2010).
- Настоящее Положение определяет задачи, функции, обязанности, ответственность и права ответственного лица за обеспечение информационной безопасности во время доступа к сети Интернет.
- Ответственное лицо за обеспечение информационной безопасности во время доступа к сети Интернет назначается приказом заведующего Учреждения и подчиняется заведующему Учреждения.
- Ответственное лицо за информационную безопасность в своей работе руководствуются настоящим Положением.

2. Основные задачи и функции ответственного за обеспечение информационной безопасности во время доступа к сети Интернет

2.1 Основными задачами ответственного за информационную безопасность во время доступа к сети Интернет являются:

2.1.1 Организация эксплуатации технических и программных средств защиты информации.

2.1.2 Текущий контроль работы средств и систем защиты информации.

2.1.3 Организация и контроль резервного копирования информации.

Функции ответственного за информационную безопасность во время доступа к сети Интернет являются

2.1.4 Разработка инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете.

2.1.5 Обучение персонала и пользователей персональным компьютером правилам безопасной обработки информации и правилам работы со средствами защиты информации.

2.1.6 Организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в Учреждение.

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

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

2.1.9 Контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК.

2.1.10 Контроль пользования Интернетом.

3. Обязанности ответственного за обеспечение информационной безопасности во время доступа к сети Интернет

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

3.2. 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.

3.4. Создавать и удалять учетные записи пользователей.

3.5. Администрировать работу сервера, размещать и классифицировать информацию на сервере.

3.6. Устанавливать по согласованию с заведующим Учреждения критерии доступа пользователей на сервер.

3.7. Формировать и представлять пароли для новых пользователей, администрировать права пользователей.

3.8. Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку компьютеров на наличие вирусов.

3.9. Выполнять регулярно резервное копирование данных на сервере, при необходимости восстанавливать потерянные или поврежденные данные.

3.10. Сообщать незамедлительно заведующему Учреждения о выявлении случаев несанкционированного доступа в Интернет.

3.11. Организовать получение сотрудниками образовательного учреждения электронных адресов и паролей для работы в сети Интернет и информационной среде образовательного учреждения;

3.12 Организовать контроль использования сети Интернет в образовательном учреждении;

3.13 Организовать контроль работы оборудования и программных средств, обеспечивающих использование Реестра безопасных образовательных сайтов в образовательной организации;

3.14 Организовать контроль реализации в образовательном учреждении методических рекомендаций по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;

3.15 Систематически повышать свою профессиональную квалификацию по направлению «Организация защиты детей от видов информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательных организациях»;

3.16 Обеспечивать информирование организаций, отвечающих за работу

технических и программных средств, об ошибках в работе оборудования и программного обеспечения;

3.17 Устанавливать аппаратное или программное обеспечение, осуществляющее контент-фильтрацию ресурсов сети Интернет на основе Реестра безопасных образовательных сайтов Перечень.

3.18 Обеспечивать контроль работы контентной-фильтрации на постоянной основе.

3.19 Еженедельно проверять точки доступа к сети Интернет на предмет выявления обращений к ресурсам, содержащим информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;

3.20 При обнаружении обращений ресурсам, н содержащим информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, немедленно сообщать заведующему Учреждения с целью своевременного принятия незамедлительных мер к исключению доступа к подобной информации.

3.21 Своевременно вести документацию:

3.20. Соблюдать правила и нормы охраны труда, техники безопасности и противопожарной защиты, правила использования сети Интернете.

4. Права

4.1. Готовить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов.

5. Ответственность

5.1 Возлагается персональная ответственность за качество проводимых работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определёнными настоящим Положением.

5.2 Несет ответственность за ограничение доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательной организации.