

Принято на заседании общего собрания
МКДОУ «Детский сад №8» ИМОСК

Протокол №1 от 09.01.2024г.

УТВЕРЖДЕНО:
Заведующий МКДОУ
«Детский сад №8» ИМОСК
Е.И.Колосова
Приказ от 09.01.2024г. №11

Принято с учётом мнения
выборных представителей родителей
(законных представителей)
несовершеннолетних воспитанников
МКДОУ «Детский сад №8» ИМОСК
входящих в родительский комитет
Протокол №1 от 09.01.2024г

Положение о Политике информационной безопасности в муниципальном казённом дошкольном образовательном учреждении «Детский сад №8 » Изобильненского муниципального округа Ставропольского края

1. Общие положения.

1. Политика информационной безопасности разработана в соответствии с Федеральным законом от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 29.12.2010г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Федеральным законом от 29.12.2012г. № 273-ФЗ «Об образовании в Российской Федерации», Концепцией информационной безопасности детей, утвержденной Распоряжением Правительства Российской Федерации от 28.04.2023г. № 1105-р, Концепцией формирования и развития культуры информационной безопасности граждан Российской Федерации, утвержденной Распоряжением Правительства РФ от 22.12.2022 № 4088-р, , Основами государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей, утвержденными Указом Президента РФ от 9 ноября 2022 г. № 809, Стратегией комплексной безопасности детей в Российской Федерации на период до 2030 года, утвержденной Указом Президента Российской Федерации от 17.05.2023 № 358, Планом мероприятий по реализации Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года, утвержденным Распоряжением Правительства РФ от 17.11.2023 № 3233-р, Планом мероприятий, направленных на обеспечение информационной безопасности детей, на 2021-2027 годы, утвержденным приказом Министерства связи и массовых коммуникаций от 01.12.2020г. № 644, с учетом методических рекомендаций по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей.

2. Настоящая Политика информационной безопасности является документом, направленным на выработку единого согласованного подхода по ограничению доступа воспитанников к негативной информации в ДОУ .

3. Основными целями Политики информационной безопасности являются:

а) формирование у всех участников образовательного процесса в ДОУ (обучающихся, родителей (законных представителей), педагогических работников) единообразного понимания политики организации и реализации защитных механизмов по ограничению доступа воспитанников к видам информации, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;

б) выработка единого согласованного подхода по ограничению доступа воспитанников к негативной информации в ДОУ

в) обобщение и разъяснение основных требований законодательства РФ в области информационной безопасности, применяемых в ДОУ

4. Для достижения поставленных целей устанавливаются следующие задачи Политики информационной безопасности:

а) закрепление основных принципов в области информационной безопасности;

б) определение области применения Политики информационной безопасности и круга лиц, попадающих под ее действие;

в) установление перечня реализуемых мероприятий, стандартов и процедур, и порядка их выполнения (применения);

г) установление ответственности работников ДОУ за несоблюдение требований Политики информационной безопасности.

2. Используемые в политике понятия и определения

Негативная информация - Виды информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (раздел «Термины и сокращения», Методические рекомендации 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, утверждённые Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

Единый реестр - Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено (раздел «Термины и сокращения», Методические рекомендации по ограничению в образовательных учреждениях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, утверждённые Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

Реестр НСОР - Реестр несовместимых с задачами образования ресурсов (раздел «Термины и сокращения», Методические рекомендации по ограничению в образовательных учреждениях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, утверждённые Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

РБОС - Перечень сайтов в сети "Интернет", рекомендованных и одобренных для использования в образовательном процессе. Реестр безопасных образовательных сайтов реализуется Временной комиссией Совета Федерации по развитию информационного общества (раздел «Термины и сокращения», Методические

рекомендации по ограничению в образовательных учреждениях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, утверждённые Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

СКФ - Система контентной фильтрации, обеспечивающая ограничение доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (раздел «Термины и сокращения», Методические рекомендации по ограничению в образовательных учреждениях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, утверждённые Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

Черный список – Контентная фильтрация и ограничение доступа обучающихся к информации, включенной в Перечень видов информации, запрещенной к распространению посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (раздел «Термины и сокращения», Методические рекомендации по ограничению в образовательных учреждениях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, утверждённые Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

Белый список – Контентная фильтрация и предоставление доступа обучающимся к сайтам в сети «Интернет», включенным в реестр безопасных образовательных сайтов (раздел «Термины и сокращения», Методические рекомендации по ограничению в образовательных учреждениях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, утверждённые Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

Портал система контентной фильтрации – Информационный портал Временной комиссии Совета Федерации по развитию информационного общества по реализации методических рекомендаций по ограничению в образовательных учреждениях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, по адресу www.единыйурок.рф (раздел «Термины и сокращения», Методические рекомендации по ограничению в образовательных учреждениях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, утверждённые Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

Доступ детей к информации - возможность получения и использования детьми свободно распространяемой информации (ст. 2 Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.12.2022) «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Знак информационной продукции - графическое и (или) текстовое обозначение информационной продукции в соответствии с классификацией информационной продукции, предусмотренной частью 3 статьи 6 Федерального закона от 29.12.2010 № 436-ФЗ (ст. 2 Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.12.2022) «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Зрелищное мероприятие - демонстрация информационной продукции в месте, доступном для детей, и в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, в том числе посредством проведения театрально-зрелищных, культурно-просветительных и зрелищно-развлекательных мероприятий (ст. 2 Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.12.2022) «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Информационная безопасность детей - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию (ст. 2 Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.12.2022) «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Информационная продукция - предназначенные для оборота на территории Российской Федерации продукция средств массовой информации, печатная продукция, аудиовизуальная продукция на любых видах носителей, программы для электронных вычислительных машин (программы для ЭВМ) и базы данных, а также информация, распространяемая посредством зрелищных мероприятий, посредством информационно-телекоммуникационных сетей, в том числе сети "Интернет", и сетей подвижной радиотелефонной связи (ст. 2 Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.12.2022) «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Информационная продукция для детей - информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей (ст. 2 Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.12.2022) «О защите детей от информации, причиняющей вред их здоровью и развитию»)

Информация, причиняющая вред здоровью и (или) развитию детей, - информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с частями 2 и 3 статьи 5 Федерального закона от 29.12.2010 № 436-ФЗ (ст. 2 Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.12.2022) «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Классификация информационной продукции - распределение информационной продукции в зависимости от ее тематики, жанра, содержания и художественного оформления по возрастным категориям детей в порядке, установленном статьей 6 Федерального закона от 29.12.2010 № 436-ФЗ (ст. 2 Федерального закона от 29.12.2010 № 436-ФЗ (ред. от 29.12.2022) «О защите детей от информации, причиняющей вред их здоровью и развитию»).

3. Основные принципы деятельности организации в области информационной безопасности

3.1. Исходя из понимания информационной безопасности детей как защиты ребёнка от дестабилизирующего воздействия информационной продукции и создания условий информационной среды для позитивной социализации и индивидуализации, оптимального социального, личностного, познавательного и

физического развития, сохранения психического и психологического здоровья и благополучия, а также формирования позитивного мировосприятия, Политика информационной безопасности основывается на конституционных гарантиях равенства прав и свобод граждан и реализуется в соответствии со следующими принципами:

- а) ответственность ДООУ за соблюдение законных интересов, воспитанников в информационной сфере;
- б) необходимость формирования у воспитанников умения ориентироваться в современной информационной среде;
- в) воспитание у воспитанников навыков самостоятельного и критического мышления;
- г) поддержка творческой деятельности воспитанников в целях их самореализации в информационной среде;
- д) создание условий для формирования в информационной среде благоприятной атмосферы для воспитанников вне зависимости от их социального положения, религиозной и этнической принадлежности;
- е) открытость и взаимодействие с другой информационной культурой и традициями, формирование у воспитанников объективного представления о российской культуре как неотъемлемой части мировой цивилизации.

3.2. В своей деятельности в области информационной безопасности ДООУ руководствуется следующими принципами:

- а) принцип объединения усилий всех заинтересованных сторон, основанный на общности целей всех субъектов обеспечения информационной безопасности личности о воспитанника (педагогические работники, родители (законные представители) воспитанника), что создает необходимые предпосылки для объединения усилий и выработки совместных действий в интересах детей;
- б) принцип непрерывности, последовательности и комплексности, предполагающий формирование исчерпывающего комплекса мер по защите воспитанника от вредной информации и последовательную, с учетом возрастных и психологических особенностей воспитанника, реализацию во всех точках информационного пространства на территории ДООУ, применяя все виды и формы защиты в полном объеме;
- в) принцип открытости, который предполагает широкое информационное сопровождение деятельности по обеспечению информационной безопасности воспитанника, создание информационных ресурсов и методических рекомендаций для родителей (законных представителей), педагогических работников по проведению профилактической деятельности;
- г) принцип возможности создания для ребенка инфобезопасной среды дома и в образовательном учреждении, основанный на необходимости создать информационно-образовательную среду, дополнить ее аппаратными, программными и организационными средствами и способами защиты от негативной информации в целях обеспечения безопасности и защиты личностной информационной среды воспитанника, создания условий для наиболее полноценного развития и реализации его индивидуальных способностей и возможностей.

4. Область применения Политики информационной безопасности и круг лиц, попадающих под ее действие

4.1. Основным кругом лиц, попадающих под действие Политики информационной безопасности, являются работники ДООУ, находящиеся в трудовых отношениях, вне

зависимости от занимаемой должности и выполняемых функций и родители (законные представители) воспитанников.

4.2. Положение Политики информационной безопасности может распространяться и на иных физических и (или) юридических лиц, с которыми ДООУ вступает в договорные отношения, в случае, если это закреплено в договорах, заключаемых ДООУ с такими лицами.

5. Должностные лица учреждения, ответственные за реализацию Политики информационной безопасности

5.1. Руководитель или назначенное Приказом должностное лицо является ответственным за организацию всех мероприятий, направленных на реализацию информационной безопасности в ДООУ .

5.2. Основные обязанности лица, ответственного за реализацию Политики информационной безопасности:

- 1) подготовка рекомендаций для принятия решений по вопросам информационной безопасности;
- 2) подготовка предложений, направленных на устранение причин и условий, порождающих риск нарушений информационной безопасности;
- 3) разработка и утверждение локальных нормативных актов, направленных на реализацию мер по обеспечению информационной безопасности;
- 4) проведение контрольных мероприятий, направленных на выявление правонарушений работниками муниципальных образовательных учреждений, родителями (законными представителями);
- 5) прием и рассмотрение сообщений о случаях нарушений Политики информационной безопасности работниками, родителями (законными представителями), контрагентами организации или иными лицами;
- 6) проведение просветительских мероприятий и индивидуального консультирования работников, воспитанников и родителей (законных представителей);
- 7) организация текущего контроля за соблюдением выполнения требований Политики информационной безопасности;
- 8) обеспечение бесперебойного функционирования системы контентной фильтрации;
- 9) осуществление контроля (мониторинга) функционирования системы контентной фильтрации;
- 10) постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов ДООУ ;
- 11) разработка и внедрение и контроль эффективности защитных мер;
- 12) оказание содействия уполномоченным представителям контрольно-надзорных и правоохранительных органов при проведении ими инспекционных проверок деятельности ДООУ по вопросам организации информационной безопасности на территории ДООУ .

6. Обязанности работников учреждения

6.1. Все работники вне зависимости от должности и стажа работы в связи с исполнением своих должностных обязанностей должны:

- 1) руководствоваться Положением Политики информационной безопасности и неукоснительно соблюдать ее принципы и требования;

2) воздерживаться от поведения, которое может быть истолковано окружающими как готовность совершить или участвовать в совершении правонарушения от имени ДОУ

3) незамедлительно информировать непосредственного руководителя о случаях нарушения информационной безопасности;

4) сообщить руководителю о возможности возникновения или уже возникшем у работника конфликте интересов в области информационной безопасности.

7. Направления, реализуемые учреждением по обеспечению информационной безопасности

7.1. ДОУ должно осуществлять меры по обеспечению безопасности личной информационной среды воспитанника в рамках следующих направлений:

1) правовое обеспечение информационной безопасности - разработка нормативных актов, правил, процедур и мероприятий, обеспечивающих защиту личной информационной среды воспитанника на законодательной и правовой основе для реализации основных принципов Политики информационной безопасности;

2) нравственный и этический контроль - соблюдение воспитанниками и работниками учреждения при осуществлении информационной деятельности норм и правил поведения в обществе, а также сетевой культуры и этики;

3) защита психики и здоровья ребенка - направленность мер на актуализацию потребности воспитанников в хорошем здоровье, физическом благополучии как средств достижения жизненно важных ценностей, снижение и профилактика компьютерной и интернет-зависимости среди воспитанников, педагогическая и психологическая помощь в вопросах уменьшения информационных опасностей в жизнедеятельности воспитанников;

4) организационная защита - регламентация информационной деятельности воспитанников, контроль использования сетевых сервисов и сообществ, исключающие или ослабляющие нанесение вреда воспитанника;

5) воспитательные меры по обеспечению информационной безопасности - формирование у воспитанников культуры информационной безопасности, ответственности за осуществленные действия в информационном пространстве, воспитание и укрепление духовно-нравственных ценностей и патриотизма;

б) техническое и программное обеспечение информационной безопасности - использование различных аппаратных и программных средств, препятствующих нанесению материального или морального ущерба личной информации, программ родительского контроля, сетевых фильтров, технических средств защиты информации.

8. Организация системы ограничения обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования

8.1. ДОУ обязано использовать многоформатную модель реализации системы контентной фильтрации.

8.2. Технология организации системы ограничения воспитанников к негативной информации не может меняться чаще, чем раз в календарный год, с целью исключения практики смены технологий фильтрации ДОУ при проведении проверок уполномоченными органами и введения их в заблуждение о качестве организации системы контентной фильтрации.

8.3. При использовании технологии контентной фильтрации и ограничении доступа воспитанников к негативной информации соблюдаются следующие положения:

1) при возможности персональной идентификации каждого воспитанников при осуществлении его доступа в сеть «Интернет», должен осуществляться доступ воспитанника к информационной продукции в соответствии с классификацией информационной продукции, предусмотренной Федеральным законом № 436-ФЗ; 2) при отсутствии возможности персональной идентификации каждого воспитанника при осуществлении его доступа в сеть «Интернет», осуществляется доступ обучающегося к информационной продукции для детей, достигших возраста шести лет.

8.4. Педагогические работники имеют право отключать систему контентной фильтрации на устройствах, предоставленных педагогическому работнику, после осуществления образовательного процесса и отсутствия несовершеннолетних на территории ДООУ с письменного согласия руководителя ДООУ с указанием или пояснением целей и временного срока отключения системы контентной фильтрации.

8.5. Системы контентной фильтрации, используемые ДООУ, должны соответствовать ряду требований.

8.6. Применяемые при разработке и использовании интерфейсов технологии, стандарты и спецификации должны соответствовать нормативно установленным и общепринятым стандартам и требованиям в области информационных технологий и программного обеспечения.

8.7. При использовании сетевых протоколов передачи данных рекомендуется придерживаться следующих спецификаций:

1) протокол передачи гипертекста версии 1.11 - RFC 2616;

2) расширенный протокол передачи гипертекста версии 1.1 с обеспечением безопасности транспортного уровня;

3) протокол защищенных соединений (SSL) версии 3 - RFC 5246; 4) протоколы использования системы поддержки пространства имен - FC 1035.

8.9. При описании данных, а также информации о данных, их составе и структуре, содержании, формате представления, методах доступа и требуемых для этого полномочиях пользователей, о месте хранения, источнике, владельце и др. (далее - метаданные) и используемых наборах символов, применяемых в процессе информационного обмена, рекомендуется придерживаться следующих спецификаций:

1) расширяемый язык разметки XML-набор стандартов Консорциума Всемирной паутины;

2) расширяемый язык описания схем данных (XML Schema) версии не ниже 1.0.

8.10. Описания разрабатываемых электронных сервисов и описания схем данных, согласно базовому профилю интероперабельности версии 1.1, рекомендуется создавать в кодировке UTF-8 или UTF-16 (с указанием этой кодировки в заголовке соответствующего описания).

8.11. Аутентификацию рекомендуется обеспечить на основе сертификатов PKI в формате X.509.

8.12. В зависимости от технологии система контентной фильтрации должна обеспечивать следующие основные функции:

1) осуществлять в режиме реального времени анализ сайтов в сети «Интернет», к которым обращаются пользователи, на предмет отсутствия информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;

- 2) пропускать, блокировать или модифицировать информацию от сайта в сети «Интернет» к пользователю в зависимости от результатов проверки;
- 3) автоматически передавать данные во внешнюю систему о сайте в сети «Интернет», информация из которого удовлетворяет заданным правилам;
- 4) собирать статистику фильтрации.

8.13. Система контентной фильтрации должна обеспечивать возможность анализа информационной продукции в любой форме и виде, в том числе возможность:

- 1) семантического и морфологического анализа информации сайтов, получаемых по HTTP протоколу, на основе списков запрещенных слов, словообразований и словосочетаний, содержащих информацию, причиняющую вред здоровью и (или) развитию детей, а также не соответствующую задачам образования, а также сочетаний слов, образующих совокупности запрещенных выражений. Информация сайтов должна интерпретироваться строго согласно стандартам на протокол передачи гипертекста и язык разметки гипертекста, в том числе должна корректно определяться кодировка передаваемых данных;
- 2) анализа поисковых HTTP-запросов путем разбора запроса, сформированного поисковыми машинами, и сравнением составных частей запроса со словарем слов, словосочетаний и словообразований, содержащих информацию, причиняющую вред здоровью и (или) развитию детей, а также не соответствующую задачам образования. Система контентной фильтрации должна поддерживать множество категорий запрещенных слов, словообразований и словосочетаний.

8.14. Система контентной фильтрации должна обеспечивать сопоставление категории сайта в сети «Интернет» с возрастной категорией пользователя и принимать решение о доступе пользователя к информации в соответствии с классификацией информационной продукции.

8.15. Система контентной фильтрации не должна предоставлять возможности для пропуска пользователя к информации сайта в сети «Интернет», содержащего информацию, причиняющую вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

8.16. Система контентной фильтрации должна обеспечивать возможность по результатам анализа сайтов:

- 1) блокировки URL-адреса сайта, запрашиваемой по HTTP протоколу;
- 2) отображение специальной страницы блокировки в случае блокировки URL-адреса сайта;
- 3) блокировки части информации от сайта, запрашиваемой по HTTP протоколу, и пропуск только не заблокированных частей пользователю;
- 4) метод принудительного включения безопасного поиска в поисковых системах путем добавления аргументов "&family=yes&", "&safe=yes&" и других в зависимости от поисковых систем.

8.17. Система контентной фильтрации должна обеспечивать сбор статистики фильтрации, включая:

- 1) время;
- 2) IP-адрес, с которого произошло обращение;
- 3) образовательное учреждение (по соответствию IP-адреса);
- 4) URL сайта или домен системы DNS, к которому было произведено обращение, либо ключевые слова, по которым было заблокировано обращение, если обращение было заблокировано методом поисковой или контентной фильтрации;
- 5) вид

фильтрации, согласно которому обращение было заблокировано, если обращение было заблокировано;

б) подтверждение пользователя, если он был предупрежден о потенциально опасной информации.

8.18. Система контентной фильтрации должна обеспечивать хранение статистики в течение срока, устанавливаемого соответствующими нормативными документами, и возможность передачи статистики во внешние системы в соответствии с установленными требованиями к взаимодействию.

8.19. Система контентной фильтрации должна обеспечивать автоматическое обновление конфигурации система контентной фильтрации при изменении параметров настройки система контентной фильтрации. Параметрами система контентной фильтрации являются:

- 1) пороговая величина блокировки сайта на основе семантического и морфологического анализа;
- 2) адрес специальной страницы блокировки;
- 3) адрес специальной страницы блокировки поисковых HTTP-запросов;
- 4) адрес специальной страницы предупреждения с возможностью пропуска информации от сайта.

8.20. Система контентной фильтрации должна обеспечивать автоматическое обновление конфигурации (правил) фильтрации при изменении информации в РБОС. Обновление должно осуществляться не более чем через 3 рабочих дня после изменений в РБОС списков URL адресов сайтов.

9. Общественный контроль за обеспечением защиты детей от видов информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования

9.1. Согласно статье 21 Федерального закона № 436-ФЗ контроль за соблюдением требований данного закона вправе осуществлять общественные объединения, зарегистрированные в установленном федеральным законом порядке, и иные некоммерческие организации в соответствии с их уставами, а также граждане.

9.2. ДОУ рекомендуется создавать советы по обеспечению информационной безопасности обучающихся, в деятельность которых вовлекаются педагогические работники, родители (законные представители) обучающихся, а также представители органов власти и общественных организаций.

9.3. Члены совета по обеспечению информационной безопасности воспитанников могут осуществлять не только регулярный мониторинг качества системы контентной фильтрации в ДОУ, но и принимать участие в реализации плана мероприятий ДОУ по обеспечению защиты воспитанников от негативной информации.

10. Система организационно-административных мероприятий, направленных на защиту детей от видов информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования

10.1. Организационно-административные мероприятия, направленные на защиту детей от видов информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, включают:

- 1) проведение ежегодного мониторинга качества работы система контентной фильтрации в ДОУ и применения организационно-административных мероприятий, направленных на защиту воспитанников от негативной информации;
- 2) организацию просветительской работы с воспитанниками и их родителями (законными представителями) в целях формирования у несовершеннолетних навыков правильного использования информации, получаемой в сети «Интернет» и из других цифровых ресурсов, предупреждения распространения своих персональных данных, а также формирования культуры информационной безопасности путем проведения мероприятий на постоянной основе;
- 3) организацию информационной работы в соответствии с письмом Минобрнауки России от 14.05.2018 № 08-1184 "О направлении информации" (вместе с Методическими рекомендациями о размещении на информационных стендах, официальных интернетсайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети «Интернет»);
- 4) оказание методической поддержки ответственным лицам и педагогическим работникам ДОУ , посвященной вопросам организации защиты детей от видов информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, путем организации и проведения семинаров, лекций и конференций с участием представителей, уполномоченных на проведение проверок образовательных организаций в части работы система контентной фильтрации, а также информирования о курсах повышения квалификации ответственных лиц и педагогических работников по вопросам обеспечения медиабезопасности образовательной среды.

10.1. Организационно-административные мероприятия, реализуемые ДОУ , направленные на защиту детей от видов информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, включают:

- 1) обеспечение защиты воспитанников от негативной информации посредством использования система контентной фильтрации при доступе к сети «Интернет» в ДОУ ;
- 2) проведение до 30 августа ежегодного мониторинга качества работы системы контентной фильтрации и применения организационно-административных мероприятий, направленных на защиту воспитанников от негативной информации;
- 3) обеспечение контроля за исполнением Положения об ограничении доступа воспитанников к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, определяющего в ДОУ основные аспекты организации работы системы контентной фильтрации, технологию, формат (форматы) реализации системы контентной фильтрации и содержащего:
 - а) приказ о назначении ответственного лица в ДОУ за обеспечение безопасного доступа к сети «Интернет», включая должностную инструкцию ответственного лица в муниципальном образовательном учреждении за обеспечение безопасного доступа к сети «Интернет»;

б) порядок проведения проверки эффективности использования систем контентной фильтрации в ДООУ включающий типовой акт проверки системы контентной фильтрации в ДООУ

в) план мероприятий по обеспечению информационной безопасности в ДООУ;

г) приказ о порядке использования на территории ДООУ персональных устройств, имеющих возможность выхода в сеть «Интернет»

4) организация просветительской работы с воспитанниками и их родителями (законными представителями) в целях формирования у несовершеннолетних навыков правильного использования информации, получаемой в сети «Интернет» и из других цифровых ресурсов, предупреждения распространения своих персональных данных, формирования культуры информационной безопасности путем реализации программ и проведения мероприятий на постоянной основе;

5) направление на повышение квалификации ответственных лиц и педагогических работников ДООУ по вопросам обеспечения медиабезопасности образовательной среды;

б) организация ежеквартального мониторинга изменения федерального законодательства и нормативно-правовых актов федерального уровня, связанных с защитой детей от видов информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, и предоставление ответственным сотрудникам за организацию в ДООУ системы контентной фильтрации соответствующих актуальных федеральных законов нормативно-правовых актов федерального уровня;

10) проведение мониторинга использования сайтов в образовательном процессе в целях обучения и воспитания воспитанника в ДООУ до 30 августа ежегодно;

11) обеспечение условий отсутствия информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, на официальных сайтах муниципальных образовательных учреждений и сайтах, задействованных в осуществлении образовательной деятельности образовательной организации.

11. Порядок использования персональных устройств обучающихся, имеющих возможность выхода в сеть «Интернет»

11. 1.Порядок использования на территории ДООУ персональных устройств, имеющих возможность выхода в сеть «Интернет», оформляется в форме Приказа о порядке использования на территории муниципального образовательного учреждения персональных устройств, имеющих возможность выхода в сеть «Интернет», согласия родителей с порядком использования персональных устройств, имеющих возможность в сеть «Интернет» на территории ДООУ .

11. 2.Приказ размещается на сайте муниципального образовательного учреждения в открытом доступе в соответствии с приказом Федеральной службы по надзору в сфере образования и науки от 04.08.2023г. № 1493 «Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети "Интернет" и формату представления информации».