

## Политика информационной безопасности

### Глава 1. Цели и задачи внедрения Политики информационной безопасности

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 2.12.2015г. №2471-р, методическими рекомендациями 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», утверждёнными Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г., методическими рекомендациями об использовании устройств мобильной связи в общеобразовательных организациях, утвержденными Федеральной службой по надзору прав потребителей и благополучия человека, Федеральной службой по надзору в сфере образования и науки от 14.08.2019г., с учетом методических рекомендаций по основам информационной безопасности для обучающихся общеобразовательных организаций с учетом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности, разработанных во исполнение плана мероприятий по реализации Концепции информационной безопасности детей на 2018-2020 годы, утвержденного приказом Министерства связи и массовых коммуникаций от 27.03.2018г. № 88.

2. Настоящая Политика информационной безопасности является документом, направленным на выработку единого согласованного подхода по ограничению в муниципальных образовательных учреждениях, доступа обучающихся к негативной информации.

3. Основными целями Политики информационной безопасности являются:

формирование у всех участников образовательного процесса муниципальной системы образования (обучающиеся, родители, законные представители, сотрудники муниципальных образовательных учреждений) единообразного понимания политики организации и реализации защитных механизмов по ограничению доступа обучающихся к видам информации, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;

выработку единого согласованного подхода по ограничению в муниципальных образовательных учреждениях доступа, обучающихся к негативной информации;

обобщение и разъяснение основных требований законодательства РФ в области информационной безопасности, применяемых в муниципальных образовательных учреждениях.

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

закрепление основных принципов в области информационной безопасности;

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

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

закрепление ответственности сотрудников образовательных учреждений за несоблюдение требований Политики информационной политики.

## **Глава 2. Используемые в политике понятия и определения**

5. **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», утверждёнными Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

6. **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», утверждёнными Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

7. **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», утверждёнными Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

8. **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», утверждёнными Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

9. **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», утверждёнными Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

10. **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», утверждёнными Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

11. **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», утверждёнными Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

12. 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.скф.единьурок.рф](http://www.скф.единьурок.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», утверждёнными Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.05.2019г.).

13. Доступ детей к информации - возможность получения и использования детьми свободно распространяемой информации (ст. 2 Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 01.05.2019) «О защите детей от информации, причиняющей вред их здоровью»).

14. 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 01.05.2019) «О защите детей от информации, причиняющей вред их здоровью»).

15. 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 01.05.2019) «О защите детей от информации, причиняющей вред их здоровью»).

16. 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 01.05.2019) «О защите детей от информации, причиняющей вред их здоровью»).

17. 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 01.05.2019) «О защите детей от информации, причиняющей вред их здоровью»).

18. 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 01.05.2019) «О защите детей от информации, причиняющей вред их здоровью»).

19. 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 настоящим Федеральным законом (ст. 2 Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 01.05.2019) «О защите детей от информации, причиняющей вред их здоровью»).

20. Информация порнографического характера - информация, представляемая в виде натуралистических изображения или описания половых органов человека и (или) полового сношения либо сопоставимого с половым сношением действия сексуального характера, в

том числе такого действия, совершаемого в отношении животного (ст. 2 Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 01.05.2019) «О защите детей от информации, причиняющей вред их здоровью»);

21. Классификация информационной продукции - распределение информационной продукции в зависимости от ее тематики, жанра, содержания и художественного оформления по возрастным категориям детей в порядке, установленном Федеральным законом от 29.12.2010 № 436-ФЗ (ст. 2 Федерального закона от 29.12.2010 № 436-ФЗ (ред. от 01.05.2019) «О защите детей от информации, причиняющей вред их здоровью»).

### **Глава 3. Основные принципы деятельности организации в области информационной безопасности**

22. Исходя из понимания информационной безопасности детей как защиты ребенка 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:

признание обучающихся равноправными участниками процесса формирования информационного общества;

ответственность образовательной организации за соблюдение законных интересов, обучающихся в информационной сфере;

необходимость формирования у обучающихся умения ориентироваться в современной информационной среде;

воспитание у обучающихся навыков самостоятельного и критического мышления;

обучение обучающихся медиаграмотности;

поддержка творческой деятельности обучающихся в целях их самореализации в информационной среде;

создание условий для формирования в информационной среде благоприятной атмосферы для обучающихся вне зависимости от их социального положения, религиозной и этнической принадлежности;

открытость и взаимодействие с другой информационной культурой и традициями, формирование у детей объективного представления о российской культуре как неотъемлемой части мировой цивилизации.

23. В своей деятельности в области информационной безопасности муниципальные образовательные учреждения руководствуются следующими принципами:

**принцип объединения усилий всех заинтересованных сторон.** Принцип основывается на общности целей всех субъектов обеспечения информационной безопасности личности обучающегося (сотрудники, родители или законные представители обучающегося). Общность целей создает необходимые предпосылки для объединения усилий и выработки совместных действий в интересах детей;

**принцип непрерывности, последовательности и комплексности.** Принцип предполагает формирование исчерпывающего комплекса мер по защите обучающегося от вредной информации и последовательную, с учетом возрастных и психологических особенностей обучающегося реализацию во всех точках информационного пространства на территории образовательного учреждения. Для защиты обучающихся от вредной информации должны применяться все виды и формы защиты в полном объеме. Недопустимо применять отдельные формы или технические средства;

**принцип открытости** предполагает широкое информационное сопровождение деятельности по обеспечению информационной безопасности обучающегося, создание информационных ресурсов и методических рекомендаций для родителей, учителей по проведению профилактической деятельности;

**принцип возможности создания для ребенка инфобезопасной среды дома и в учреждении.** В соответствии с этим принципом необходимо создать информационно-

образовательную среду, дополнить ее аппаратными, программными и организационными средствами и способами защиты от негативной информации. Инфобезопасная среда должна обеспечивать безопасность и защиту личностной информационной среды обучающегося в целях создания условий для наиболее полноценного развития, и реализации индивидуальных способностей и возможностей.

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

24. Основным кругом лиц, попадающих под действие Политики информационной безопасности, являются работники муниципальных образовательных учреждений, находящиеся в трудовых отношениях, вне зависимости от занимаемой должности и выполняемых функций; обучающиеся; родители или законные представители обучающихся.

25. Положения настоящей Политики информационной безопасности могут распространяться на иных физических и (или) юридических лиц, с которыми муниципальные образовательные учреждения вступают в договорные отношения, в случае если это закреплено в договорах, заключаемых муниципальными образовательными учреждениями с такими лицами.

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

26. Руководитель или назначенное Приказом должностное лицо муниципального образовательного учреждения является ответственным за организацию всех мероприятий, направленных на реализацию информационной безопасности в муниципальном образовательном учреждении.

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

- подготовка рекомендаций для принятия решений по вопросам информационной безопасности;

- подготовка предложений, направленных на устранение причин и условий, порождающих риск нарушений информационной безопасности;

- разработка и утверждение локальных нормативных актов, направленных на реализацию мер по обеспечению информационной безопасности;

- проведение контрольных мероприятий, направленных на выявление правонарушений работниками муниципальных образовательных учреждений, обучающимися и родителями или законными представителями;

- прием и рассмотрение сообщений о случаях нарушений Политики информационной безопасности работниками, обучающимися, родителями или законными представителями, контрагентами организации или иными лицами;

- проведение обучающих мероприятий по вопросам профилактики и индивидуального консультирования работников, обучающихся и родителей или законных представителей;

- организация текущего контроля за соблюдением выполнения требований Политики информационной безопасности;

  - обеспечение бесперебойного функционирования системы контентной фильтрации;

  - осуществление контроля (мониторинга) функционирования системы контентной фильтрации;

  - постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов образовательной организации;

  - разработка и внедрение защитных мер;

  - контроль эффективности принимаемых защитных мер;

  - оказание содействия уполномоченным представителям контрольно-надзорных и правоохранительных органов при проведении ими инспекционных проверок деятельности образовательного учреждения по вопросам организации информационной безопасности на территории образовательного учреждения.

## **Глава 6. Обязанности работников учреждения**

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

руководствоваться положениями настоящей Политики информационной безопасности и неукоснительно соблюдать ее принципы и требования;

воздерживаться от поведения, которое может быть истолковано окружающими как готовность совершить или участвовать в совершении правонарушения от имени образовательного учреждения;

незамедлительно информировать непосредственного руководителя о случаях нарушения информационной безопасности;

сообщить руководителю о возможности возникновения либо возникшем у работника конфликте интересов в области информационной безопасности.

## **Глава 7. Направления, реализуемые учреждением по обеспечению информационной безопасности**

29. Муниципальные образовательные учреждения должны осуществлять меры по обеспечению безопасности личной информационной среды обучающегося в рамках следующих направлений:

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

**нравственный и этический контроль** - соблюдение обучающимися, сотрудниками Учреждения при осуществлении информационной деятельности норм и правил поведения в обществе, а также сетевой культуры и этики;

**защита психики и здоровья ребенка.** Меры направлены на актуализацию потребности обучающихся в хорошем здоровье, физическом благополучии как средств достижения жизненно важных ценностей, снижение и профилактика компьютерной и интернет-зависимости среди обучающихся, педагогическая и психологическая помощь в вопросах уменьшения информационных опасностей в жизнедеятельности обучающихся;

**организационная защита** - регламентация информационной деятельности обучающихся, контроль использования сетевых сервисов и сообществ, исключающие или ослабляющие нанесение вреда обучающемуся;

**воспитательные меры по обеспечению информационной безопасности.** Формирование у обучающегося культуры безопасности, ответственность за осуществленные действия в информационном пространстве, воспитание и укрепление духовно-нравственных ценностей, патриотизм;

**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.

## **Глава 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**

30. Муниципальные образовательные учреждения обязаны использовать многоформатную модель реализации системы контентной фильтрации.

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

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

1) при возможности персональной идентификации каждого обучающегося при

осуществлении его доступа в сеть «Интернет», должен осуществляться доступ обучающегося к информационной продукции в соответствии с классификацией информационной продукции, предусмотренной Федеральным законом №436-ФЗ;

2) при отсутствии возможности персональной идентификации каждого обучающегося при осуществлении его доступа в сеть «Интернет», осуществляется доступ обучающегося к информационной продукции для детей, достигших возраста шести лет.

33. Педагогические работники имеют право отключать систему контентной фильтрации на устройствах, предоставленных педагогическому работнику, после осуществления образовательного процесса и отсутствия несовершеннолетних на территории муниципального образовательного учреждения, после получения письменного согласия от руководителя или заместителя руководителя образовательного учреждения с указанием или пояснением целей отключения системы контентной фильтрации и временных сроках отключения системы контентной фильтрации.

34. В муниципальном образовательном учреждении ведется журнал (Приложение № 1) работы системы контентной фильтрации, в который включаются сведения об отключении педагогическим работником на устройстве системы контентной фильтрации.

35. Системы контентной фильтрации, используемые муниципальными образовательными учреждениями, должны соответствовать ряду требований.

36. 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.

37. 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.

38. 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.

39. 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).

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

41. 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 на сайтах в сети «Интернет» 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 к пользователю в зависимости от результатов проверки;

3) автоматически передавать данные во внешнюю систему о сайте, информация из которого удовлетворяет заданным правилам;

4) собирать статистику фильтрации.

42. Система контентной фильтрации должна обеспечивать возможность анализа

информационной продукции в любой форме и виде, в частности 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.

43. 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.

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

45. 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.

46. 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;

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

47. 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.

48. 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.

49. 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.

#### **Глава 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**

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

51. Муниципальным образовательным учреждениям рекомендуется создать совет по обеспечению информационной безопасности обучающихся, в деятельность которого вовлечь педагогических работников, родителей (законных представителей) обучающихся и представителей органов власти и общественных организаций.

52. Члены совета по обеспечению информационной безопасности обучающихся могут осуществлять не только регулярный мониторинг качества системы контентной фильтрации в муниципальном образовательном учреждении, но и принимать участие в реализации плана мероприятий муниципального образовательного учреждения по обеспечению защиты детей от негативной информации.

#### **Глава 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**

53. Организационно-административные мероприятия, реализуемые Управлением образования Администрации города Усть-Илимска, направленные на защиту детей от видов информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования:

1) проведение ежегодного мониторинга качества работы системы контентной фильтрации в образовательных учреждениях и применения организационно-административных мероприятий, направленных на защиту детей от негативной информации;

2) организация просветительской работы с детьми и их родителями (законными представителями) по повышению культуры информационной безопасности путем реализации программ и проведения мероприятий, таких как Единый урок по безопасности в сети «Интернет», квест по цифровой грамотности «Сетевичок» и другие;

3) организация информационной работы в соответствии с письмом Минобрнауки России от 14.05.2018 N 08-1184 "О направлении информации";

4) оказание методической поддержки ответственных лиц и педагогических работников муниципальных образовательных учреждений, 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, в образовательных учреждениях путем:

организации и проведения семинаров, лекций и конференций с участием представителей уполномоченных на проведение проверок образовательных организаций в части работы системы контентной фильтрации органов;

информирования о курсах повышения квалификации ответственных лиц в образовательных учреждениях по темам «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 учреждениях» и педагогических работников по теме «Безопасное использование сайтов в

сети «Интернет» в образовательном процессе в целях обучения и воспитания обучающихся в образовательном учреждении»;

5) в качестве учредителя муниципальных образовательных учреждений обеспечить выделение муниципальным образовательным учреждениям средств для приобретения систем контентной фильтрации самостоятельно.

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

1) обеспечить защиту обучающихся от видов негативной информации для детей посредством использования система контентной фильтрации при выходе в сеть «Интернет» при доступе к сети «Интернет» из образовательного учреждения;

2) проведение до 30 августа ежегодного мониторинга качества работы системы контентной фильтрации и применения организационно-административных мероприятий, направленных на защиту детей от негативной информации для детей;

3) утвердить и обеспечить контроль исполнения Положения об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, определяющий в образовательном учреждении основные аспекты организации работы системы контентной фильтрации, технологию, формат (форматы) реализации системы контентной фильтрации и включающего:

а) приказ о назначении ответственного лица в образовательном учреждении за обеспечение безопасного доступа к сети «Интернет», включающий 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 муниципальном образовательном учреждении, включающий типовой акт проверки системы контентной фильтрации в муниципальном образовательном учреждении;

в) журнал работы системы контентной фильтрации (Приложение 2);

г) план мероприятий по обеспечению информационной безопасности в муниципальном образовательном учреждении;

д) приказ о порядке использования на территории муниципального образовательного учреждения, персональных устройств, имеющих возможность выхода в сеть «Интернет» (Приложение 3);

е) инструкции для обучающихся по обеспечению информационной безопасности при использовании сети «Интернет» для размещения в учебных кабинетах, в которых осуществляется доступ в сеть «Интернет»;

ж) внесение изменений в должностные инструкции педагогических работников об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, включая порядок осуществления контроля педагогическими работниками использования, обучающимися сети «Интернет»;

4) организация просветительской работы с детьми и их родителями (законными представителями) по повышению культуры информационной безопасности путем реализации программ и проведения мероприятий, таких как Единый урок по безопасности в сети «Интернет», квест по цифровой грамотности «Сетевичок» и другие;

5) направление на повышение квалификации ответственных лиц в образовательном учреждении по темам «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 учреждениях» и педагогических работников по теме «Безопасное использование сайтов в сети «Интернет» в образовательном процессе в целях обучения и воспитания обучающихся в образовательной организации»;

б) организация информационной работы в соответствии с письмом Минобрнауки России от 14.05.2018 №08-1184 «О направлении информации»;

7) 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 муниципальном образовательном учреждении системы контентной фильтрации соответствующих актуальных федеральных законов нормативно-правовых актов федерального уровня;

8) обеспечить на мобильных устройствах, принадлежащих муниципальному образовательному учреждению, подключение функции «Родительский контроль» или установку специализированного программного обеспечения, позволяющего исключить возможность доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;

9) заключить договор (контракт) с поставщиком системы контентной фильтрации при условии наличия в договоре (контракте) положений об ответственности и обязательстве поставщика система контентной фильтрации в виде компенсации понесенного ущерба за ненадлежащее оказание услуги.

10) обеспечить мониторинг использования сайтов в образовательном процессе в целях обучения и воспитания, обучающихся в муниципальном образовательном учреждении до 30 августа ежегодно;

11) обеспечить отсутствие 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 реализации образовательной деятельности образовательной организации, включая системы электронных дневников и дистанционного обучения.

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

55. Определение порядка использования устройств мобильной связи определяется на основании Методических рекомендаций об использовании устройств мобильной связи в общеобразовательных организациях, утверждёнными Федеральной службой по надзору в сфере образования и науки и Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека от 14.08.2019г.

56. Порядок использование на территории муниципального образовательного учреждения персональных устройств, имеющих возможность выхода в сеть «Интернет», оформляется в форме Приказа (Приложение 3) о порядке использования на территории муниципального образовательного учреждения персональных устройств обучающихся, имеющих возможность выхода в сеть «Интернет», с дальнейшим получением согласия (Приложение 4) родителей (законных представителей) обучающихся о снятии ответственности с руководителя муниципального образовательного учреждения в случае предоставления обучающемуся данного устройства при посещении муниципального образовательного учреждения или согласия (Приложение 5) с порядком использования персональных устройств обучающихся, имеющих возможность в сеть «Интернет» на территории муниципального образовательного учреждения.

57. Данный Приказ размещается на сайте муниципального образовательного учреждения в открытом доступе в разделе «Документы» в соответствии с приказом Федеральной службы по надзору в сфере образования и науки от 29.05.2014г. №785 «Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления на нем информации».