УПРАВЛЕНИЕ ОБРАЗОВАНИЯ АДМИНИСТРАЦИИ НГО

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
Г И М Н А З И Я № 41
(МАОУ «Гимназия № 41»)

П Р И К А З

« 27 » июня 2023 г. № 73

г. Новоуральск

Об обеспечении информационной безопасности и противодействии экстремистской деятельности в 2023-2024 учебном году

На основании Федеральных законов от 27 июля 2006 г. №152-ФЗ «О персональных данных» (с изменениями на 31 декабря 2017 года), от 27 июля 2006 г. №149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 18 марта 2019 года), от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (с изменениями на 1 мая 2019 года), Постановления Правительства РФ от 1 ноября 2012 г. №_1119 «Об утверждении требований к защите персональщ,rIC данных при их обработке в информационных системах персональных данных», Приказов ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями на 23 марта 2017 года), 11 февраля 2013 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (с изменениями на 15 февраля 2017 года), Распоряжения Правительства РФ от 02.12.2015 N 2471-р «Об утверждении Концепции информационной безопасности детей», приказа Министерства образования и науки Российской Федерации от 25 июля 2002 года №114-ФЗ «О противодействии экстремистской деятельности» (с изменениями на 23 ноября 2015 года), письма Министерства образования и науки Российской Федерации от 28 апреля 2014 г. №ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет», «Правил подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации», утверждённых Министерством образования и науки Российской Федерации 11 мая 2011 г. №АФ-12/07вн, приказа Министерства связи и массовых коммуникаций Российской Федерации от 16 июня 2014 г. №161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию», письма Министерства общего и профессионального образования Свердловской области от 30.09.2015г. №02-01-82/8189 «О защите детей от информации, наносящей вред их здоровью», приказа Министерства общего и профессионального образования Свердловской области от 13.02.2015 №66-И «О проведении мониторинга эффективности использования систем контент-фильтрации в образовательных организациях Свердловской области», приказами МАОУ «Гимназия № 41» от 31.05.2023 № 63 «О назначении лица, ответственного за информационную безопасность», № 65 «О назначении лиц, ответственных за работу с документами, включенными в Федеральный список экстремистских материалов в 2023-

2024 учебном году» и с целью обеспечения информационной безопасности в МАОУ «Гимназия№ 41» в 2023-2024 учебном году,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие с 28.06.2023 года:

1) Положение об организации работы в локальной сети и сети Интернет (Приложение 1);

2) Инструкцию для сотрудников школы о порядке действий при осуществлении контроля использования обучающимися сети Интернет (Приложение 2);

3) Положение о локальной сети МАОУ «Гимназия № 41» (Приложение 3);

4) Правила работы с электронной почтой МАОУ «Гимназия № 41» (Приложение 4);

5) Положение об осуществлении антивирусной защиты в МАОУ «Гимназия № 41» (Приложение 5);

6) Инструкция по организации антивирусной защиты в МАОУ «Гимназия № 41» (Приложение 6);

7) Должностная инструкция ответственного за информационную безопасность (Приложение 7);

8) Классификатор информации, не имеющей отношения к образовательному процессу (Приложение 8).

2. Хомей Ольге Михайловне, заместителю директора по УВР, ответственной за информационную безопасность руководствоваться в работе выше перечисленными документами.

3. Контроль исполнения приказа оставляю за собой.

Директор А.В. Великов

Приложение 1
к приказу от 27.06.2023 г. № 73

Положение по организации работы в локальной сети и сети Интернет
МАОУ «Гимназия№ 41»

Общие положения

1. Настоящее Положение о работе в локальной сети и сети Интернет разработано в целях систематизации мероприятий по обслуживанию и использованию локальной сети и сети Интернет (далее - сети) в МАОУ «Гимназия № 41» и определяет регламент работы с этими сетями об$_{уч}$ающихся, сотрудников гимназии и других лиц.
2. Персональные компьютеры, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование являются собственностью МАОУ «Гимназия № 41» и предоставляются работникам и обучающимся в рамках образовательной деятельности. ПК, серверы, ПО, оборудование ЛВС и коммуникационное, пользователи образуют систему локальной компьютерной сети МАОУ «Гимназия № 41».
3. Ознакомление с Положением и его соблюдение обязательны для всех обучающихся, сотрудников гимназии, а также иных лиц, допускаемых к работе с сетями в школе.
4. Настоящее Положение имеет статус локального нормативного акта гимназии. Если нормами действующего законодательства Российской Федерации предусмотрены иные требования, чем настоящим Положением, применяются нормы действующего законодательства.
5. Использование сети Интернет в учреждении подчинено следующим принципам: соответствие образовательным целям:

– способствование гармоничному формированию и развитию личности;
– уважение закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернета;
– приобретение новых навыков и знаний;
– расширение применяемого спектра учебных и наглядных пособий; социализация личности, введение в информационное общество.

6. Целью настоящего регламента является:

– регулирование работы системного администратора и пользователей;
– распределение сетевых ресурсов коллективного пользования и поддержание необходимого уровня защиты информации, её сохранности и соблюдения прав доступа к информации;
– более эффективного использования сетевых ресурсов и уменьшения риска неправильного их использования.

7. К работе в Сети допускаются лица, прошедшие инструктаж.
8. По уровню ответственности и правам доступа к Сети пользователи разделяются на следующие категории:
   – пользователи - работники;
   – пользователи - обучающиеся.
9. В случае появления у пользователя компьютера сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере или каком-либо другом, пользователь должен немедленно сообщить об этом ответственному за информационную безопасность.

10. Пользователь-работник подключенного к Сети компьютера - сотрудник гимназии, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.

11. Пользователи-обучающиеся имеют доступ к компьютерам в компьютерных классах и компьютерам, установленных в учебных кабинетах гимназии.

12. Каждый пользователь-работник пользуется именем пользователя и паролем для входа в локальную сеть гимназии. Передача логинов и паролей для входа в локальную сеть кому-либо запрещена.

13. В случае нарушения правил пользования Сетью, связанных с администрируемым им компьютером, пользователь сообщает ответственному за информационную безопасность, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений. Если виновником нарушения является пользователь данного компьютера, ответственный за информационную безопасность имеет право отстранить виновника от пользования компьютером или принять иные меры.

14. Заместитель директора по АХР информирует пользователей обо всех плановых профилактических работах, могущих привести к частичной или полной неработоспособности Сети на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам Сети.

15. Системный администратор имеет право отключить компьютер пользователя от Сети в случае, если с данного компьютера производились попытки несанкционированного доступа к информации на других компьютерах, и в случаях других серьезных нарушений настоящего Положения.

16. Пользователь должен ознакомиться с настоящим Положением. Обязанность ознакомления пользователя с инструкцией лежит на системном администраторе и заместителе директора.

Организация использования сети Интернет в МАОУ «Гимназия №41»

17. Вопросы использования возможностей сети Интернет в образовательном процессе рассматриваются на педагогическом совете МАОУ «Гимназия № 41». Педагогический совет утверждает Правила использования сети Интернет на учебный год. Правила вводится в действие приказом директора МАОУ «Гимназия № 41».

18. Правила использования сети Интернет разрабатывается педагогическим советом МАОУ «Гимназия № 41» на основе примерного регламента самостоятельно либо с привлечением внешних экспертов, в качестве которых могут выступать:

– преподаватели других образовательных учреждений, имеющие опыт использования Интернета в образовательном процессе;

– специалисты в области информационных технологий; представители органов управления образованием; родители обучающихся.

19. При разработке правил использования сети Интернет педагогический совет руководствуется:

– законодательством Российской Федерации;

– опытом целесообразной и эффективной организации учебного процесса с использованием информационных технологий и возможностей Интернета; интересами обучающихся;

– целями образовательного процесса;

– рекомендациями профильных органов и организаций в сфере классификации ресурсов Сети.

20. Директор МАОУ «Гимназия № 41» отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в гимназии, а также за выполнение установленных правил. Для обеспечения доступа участников образовательного процесса к сети Интернет в соответствии с установленным в гимназии правилами директор МАОУ «Гимназия №41» назначает своим приказом ответственного за организацию работы с Интернетом и ограничение доступа.

21. Педагогический совет МАОУ «Гимназия № 41»:

– принимает решение о разрешении/блокировании доступа к определенным: ресурсам и (или) категориям ресурсов сети Интернет;

– определяет характер и объем информации, публикуемой в Интернет-ресурсах МАОУ «Гимназия № 41»;

– дает директору МАОУ «Гимназия № 41» рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за обеспечение доступа к ресурсам сети Интернет и контроль безопасности работы в Сети.

22. Во время уроков и других занятий в рамках учебного плана контроль использования обучающимися сети Интернет осуществляет преподаватель, ведущий занятие. При этом преподаватель:

– наблюдает за использованием компьютера и сети Интерне обучающимися;

– принимает меры по пресечению обращений к ресурсам, и имеющим отношения к образовательному процессу.

23. Во время свободного доступа обучающихся к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляют работники МАОУ «Гимназия № 41», определенные приказом директора.

24. Работник гимназии:

– наблюдает за использованием компьютера и сети Интернет обучающимися; принимает - меры по пресечению по пресечению обращений к ресурсам, не имеющих отношения к образовательному процессу;

– сообщает классному руководителю о преднамеренных попытках обучающегося осуществить обращение к ресурсам, не имеющим отношения к образовательному процессу.

25. При использовании сети Интернет в МАОУ «Гимназия № 41» обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношение к образовательному процессу. Проверка выполнения такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в МАОУ «Гимназия № 41» или предоставленного оператором услуг связи.

26. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническим средствами и программным обеспечением контентной фильтрации, в соответствии с принятыми в МАОУ «Гимназия № 41» правилами обеспечивается работником МАОУ «Гимназия № 41», назначенным его директором.

27. Принципы размещения информации на Интернет-ресурсах МАОУ «Гимназия № 41» призваны обеспечивать:

– соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;

– защиту персональных данных обучающихся, преподавателей и сотрудников; достоверность и корректность информации.

28. Персональные данные обучающихся (включая фамилию и имя, класс/год обучения, возраст, фотографию, данные о месте жительства, телефонах и пр., иные сведения личного характера) могут размещаться на Интернет-ресурсах, создаваемых МАОУ «Гимназия № 41», только с письменного согласия родителей или иных законных представителей обучающихся. Персональные данные преподавателей и сотрудников МАОУ «Гимназия № 41» размещаются на его Интернет-ресурсах только с письменного согласия лица, чьи персональные данные размещаются.

29. В информационных сообщениях о мероприятиях, размещенных на сайте МАОУ «Гимназия № 41» без уведомления и получения согласия упомянутых лиц и/или законных представителей, могут быть указаны лишь фамилия и имя обучающегося либо фамилия, имя и отчество преподавателя, сотрудника или родителя.

30. При получении согласия на размещение персональных данных представитель МАОУ «Гимназия № 41» обязан разъяснить возможные риски и последствия их опубликования. МАОУ «Гимназия № 41» не несет ответственности за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя).

Работа на компьютере

31. Перед началом работы пользователь должен:

– Включить выключатель сетевого фильтра. При включении кнопка должна начать светиться.

– Включить монитор (если выключен).

– Включить компьютер кнопкой "Power". Дождаться загрузки операционной системы (ОС);

– По завершению работы пользователь должен:

– Закрыть все открытые программы и документы, сохранив нужные изменения.

– С помощью меню "Пуск->Завершение работы" выключить компьютер и дождаться завершения работы. (Системный блок перестанет мигать и шуметь).

– Выключить монитор. Выключить сетевой фильтр.

32. Запрещено аварийно завершать работу компьютера кнопкой "Reset" или отключением от электросети. Завершение работы компьютера производится, через кнопку "Пуск->Завершение работы".

33. Запрещается самостоятельно разбирать компьютер и все его комплектующие. При возникновении неисправностей необходимо обратиться к системному администратору.

34. Все кабели, соединяющие системный блок с другими устройствами, следует вставлять и вынимать только при выключенном компьютере. Исключение составляют USB-устройства: они могут быть подключены к включенному компьютеру.

35. Подключение проектора к компьютеру осуществляется в выключенном состоянии. Выключить проектор из сети можно только после его полной остановки.

36. На компьютеры гимназии устанавливается программное обеспечение в соответствии с приобретенными лицензиями или бесплатное.

37. Запрещено самостоятельно устанавливать, удалять, деактивировать и изменять программное обеспечение и сетевые настройки на компьютере. Этим занимается только системный администратор.

38. Пользователь обязан сохранять оборудование в целости и сохранности.

39. Запрещается подвергать компьютер и периферийные устройства физическим, термическим и химическим воздействиям. (Нельзя сидеть на компьютере, проливать на него чай, кофе, просыпать семечки, ставить у батареи и других нагревательных приборов, класть книги, сумки и прочие предметы).

40. Системный блок компьютера должен стоять так, чтобы отверстия воздухозаборника не были закрыты.

41. По завершению рабочего дня компьютер необходимо выключить, и обесточить.

42. Пользователь обязан помнить свои данные для входа на свой компьютер и Сеть. В случае утраты этих данных необходимо обратиться к системному администратору.

Работа в локальной сети

43. Пользователи Сети имеют право:

– Использовать работу в сетях только в целях, непосредственно связанных с образовательным процессом;

– Использовать в работе предоставленные им сетевые ресурсы в оговоренных в рамках настоящего Положения;

– Использовать носящих исключительно игровой и развлекательный характер ресурсов сетей допускается: обучающимися - с отдельного разрешения и под контролем учителя только во внеурочное время; сотрудниками - только в нерабочее время.

– При использовании ресурсов сетей обязательным является соблюдение законодательства об интеллектуальных правах и иного применимого законодательства.

– Использовать сети обучающимися допускается только с разрешения учителя. Давший обучающемуся разрешение на работу учитель несёт ответственность за соблюдение обучающимся Положения наравне с ним. Данная норма распространяется на всех лиц, не являющихся сотрудниками ОУ, в том числе на родителей, гостей.

– Использовать ресурсы сетей во время уроков допускается только в рамках выполнения задач данных уроков. В свободное время использование обучающимися и иными лицами сетей допускается по расписанию оборудованных компьютерами кабинетов в присутствии учителя, прошедшего инструктаж по технике безопасности при работе с вычислительной техникой. Сотрудники ОУ, имеющие рабочее место, оборудованное компьютером с подключением к сети (сетям), используют сети в любое время в рамках режима работы учреждения.

– Вносить предложения по улучшению работы с ресурсом.

44. Пользователи Сети обязаны:

– Соблюдать правила работы в сети, оговоренные настоящим Положением;

– При доступе к внешним ресурсам сети, соблюдать правила, установленные системными администраторами для используемых ресурсов;

– Немедленно сообщать системному администратору сети или заместителю директора по информатизации об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящих правил кем-либо. Администратор, при необходимости, с помощью других специалистов, должен провести расследование указанных фактов и принять соответствующие меры;

– Не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы в сети;

– Обеспечивать беспрепятственный доступ системного администратора к сетевому оборудованию и компьютерам пользователей, для организации профилактических и ремонтных работ;

– Выполнять предписания системного администратора, направленные на обеспечение безопасности сети;

– В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться к заместителю директора.

45. Пользователям Сети запрещено:

– Доступ к ресурсам, несовместимым с целями и задачами образования и воспитания, запрещён.

– Разрешать посторонним лицам пользоваться вверенным им компьютером (кроме случаев подключения/отключения ресурсов, выполняемого системным администратором), без согласования с системным администратором;

– Использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей без согласования с заместителем директора;

– Самостоятельно устанавливать или удалять установленные системным администратором сетевые программы на компьютерах, подключенных к сети, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов;

– Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю;

– Вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без согласования с системным администратором, изменять настройки BIOS, а также производить загрузку рабочих станций со стороннего носителя информации;

– Самовольно подключать компьютер к сети, а также изменять IP-адрес компьютера, выданный системным администратором. Передача данных в сеть с использованием других IP адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах;

– Получать и передавать в сеть информацию, противоречащую действующему законодательству РФ и нормам морали общества, представляющую коммерческую или государственную тайну;

– Обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация;

– Использовать иные формы доступа к сети Интернет, за исключением разрешенных системным администратором: пытаться обходить межсетевой экран при соединении с сетью Интернет;

– Осуществлять попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках и сетевом взломе;

– Использовать сеть для массового распространения рекламы (спам), коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.

– Закрывать доступ к информации паролями без согласования с системным администратором.

– При использовании сетевых сервисов, предполагающих авторизацию, запрещается пользоваться чужими учётными данными.

Работа в сети Интернет

46. Пользователи используют программы для поиска информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных

обязанностей. Использование ресурсов сети Интернет разрешается только в рабочих и учебных целях, использование её ресурсов не должно потенциально угрожать школе.

47. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему санкций.

48. Сотрудникам гимназии и обучающимся, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство РФ.

49. Запрещено получать и передавать через сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.

50. Запрещено получать доступ к информационным ресурсам сети или сети Интернет, не являющихся публичными, без разрешения их собственника.

51. В школе обеспечить контентную фильтрацию ресурсов сети Интернет, вести список запрещенных сайтов. Программы для работы с Интернет должны быть сконфигурированы так, чтобы к этим сайтам нельзя было получить доступ.

52. Запрещено размещать в гостевых книгах, форумах, конференциях сообщения, содержащие грубые и оскорбительные выражения.

Ответственность

53. Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники.

54. Пользователь несёт личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в Сети и за её пределами.

55. За нарушение настоящего регламента пользователь может быть отстранен от работы с Сетью.

56. Нарушение данного регламента, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей, системы или Сети компьютеров, может повлечь административную или уголовную ответственность в соответствии с действующим законодательством.

Действия в нештатных ситуациях

57. При утрате (в том числе частично) работоспособности локальной сети или сети Интернет лицо, обнаружившее неисправность, сообщает об этом ответственному сотруднику за настройку соответствующей сети. Ответственный сотрудник за настройку сети устраняет неисправность, а при отсутствии такой возможности ставит в известность руководителя гимназии. Руководитель организует устранение неисправности - возможно, с привлечением сил и средств окружных служб или сторонних организаций.

58. При прекращении работы сети Интернет во всём учреждении ответственный сотрудник за настройку сети проверяет исправность внутришкольных подключений оборудования и настроек сети. В случае их исправности ответственный за настройку сети ставит в известность руководителя гимназии и связывается с поставщиком услуг сети Интернет с обязательной фиксацией номера заявки и последующим контролем исполнения.

59. При заражении компьютера вирусами его использование немедленно прекращается сотрудником, обнаружившим заражение. О сложившейся ситуации сообщается ответственным сотрудникам за контроль использования сетей и настройку сетей. Компьютер отключается от сетей до момента очистки от всех вирусов. Разрешение

на дальнейшее использование компьютера и подключение его к сетям даёт ответственный сотрудник за контроль над использованием сетей после соответствующей проверки.

Приложение 2
к приказу от 27.06.2023 г. № 73

Инструкция для сотрудников МАОУ «Гимназия № 41» о порядке действий при осуществлении контроля использования обучающимися сети Интернет

1. Настоящая инструкция устанавливает порядок действий сотрудников образовательных учреждений при обнаружении:

1) обращения обучающихся к контенту, не имеющему отношения к образовательному процессу;

2) отказа при обращении к контенту, имеющему отношение к образовательному процессу, вызванного техническими причинами.

2. Контроль использования обучающимися сети Интернет осуществляют:

1) во время занятия - проводящий его преподаватель и (или) работник МАОУ «Гимназия № 41», специально выделенный для помощи в проведении занятий;

2) во время использования сети Интернет для свободной работы обучающихся - сотрудник МАОУ «Гимназия № 41», назначенный руководителем ОО в установленном порядке.

3. Преподаватель:

– определяет время и место работы обучающихся в сети Интернет с учетом использования в образовательном процессе соответствующих технических возможностей, а также длительность сеанса работы одного обучающегося;

– наблюдает за использованием обучающимися компьютеров и сети Интернет; способствует осуществлению контроля объемов трафика ОУ в сети Интернет;

– запрещает дальнейшую работу обучающегося в сети Интернет на уроке (занятии) в случае нарушения им порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;

– доводит до классного руководителя информацию о нарушении обучающимся правил работы в сети Интернет;

– принимает необходимые меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

4. При обнаружении ресурса, который, по мнению преподавателя, содержит информацию, запрещенную для распространения в соответствии с законодательством Российской Федерации, или иного потенциально опасного для обучающихся контента, он сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

5. В случае отказа доступа к ресурсу, разрешенному в ОУ, преподаватель также сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

Приложение 3
к приказу от 27.06.2023 г. № 73

ПОЛОЖЕНИЕ
о локальной сети МАОУ «Гимназия № 41»
Новоуральского городского округа

Общие положения

1. Школьная локальная сеть является обеспечивающим функционирование части образовательного учреждения организационно-техническим комплексом, информационно-управленческой системы.
2. Целями настоящего Положения являются создание основы регулирования информационных процессов в сети, организация совместной работы пользователей сети.
3. Положение призвано обеспечить надежную и эффективную работу сети и каналов доступа к Интернету.
4. Соблюдение пунктов данного Положения отвечает интересам всех пользователей школьной локальной сети.

Назначение

5. Локальная сеть школы предназначена для решения задач управления и обучения на базе современных информационных технологий:
   – оперативного обмена данными между подразделениями школы; использования общих информационных ресурсов сети;
   – доступа через локальную сеть к ресурсам Интернета;
   – организации централизованного хранилища данных с различным уровнем доступа к информации.

Состав

6. Локальную сеть образуют базовые компоненты оборудования и программного обеспечения:
   – Сервер;
   – Телекоммуникационная инфраструктура: кабели, соединительные устройства;
   – Рабочие станции с необходимыми сетевыми адаптерами.
   – Системы дублирования и хранения информации.
   – Системы бесперебойного питания серверов.
   – Программное обеспечение: операционные системы;
протоколы сетевого взаимодействия; программное обеспечение коллективного доступа; программное обеспечение рабочих станций.

Принцип действия

6. Функционирование школьной локальной сети обеспечивается подключением рабочих станций к серверу с сетевой операционной системой и прикладным программным обеспечением.

7. Расширение школьной локальной сети производится путем подключения дополнительных сегментов через каналы связи.

8. Подключение к внешним информационным сетям производится через сервер, на котором установлен контент-фильтр для исключения доступа к ресурсам Интернета, несовместимыми с целями и задачами образования и воспитания учащихся.

9. Защита информации по уровням доступа производится путем администрирования файловых серверов, серверов баз данных, иных серверов и специальных организационных

Администрирование сети

10. Серверы. Администрирование серверов производится системным администратором или лицом, выполняющим его функции (далее системный администратор).

11. Уровни доступа потребителей конфиденциальной информации регламентируются и реализуются только системным администратором.

12. Отключение серверов или рабочих станций для технологических целей производится только системным администратором с обязательным предварительным уведомлением всех пользователей ресурсов данного сервера или рабочей станции.

13. При отключении серверов или устранении на них возникших неисправностей, системный администратор обязан осуществить организационно-технические мероприятия по обеспечению неразрывности рабочего процесса подразделений.

14. Установка контент-фильтров для исключения доступа к Интернет - ресурсам, несовместимым с целями и задачами образования и воспитания учащихся, производится системным администратором.

15. Создание и сопровождение телекоммуникационных каналов сети является исключительной компетенцией школы.

16. Подключение персональных компьютеров· к сети производится системным администратором.

17. Решение о подключении или реорганизации сегмента принимается системным администратором на основании заявки в соответствии с имеющимися ресурсами и техническими возможностями.

18. Изменение типологии сети самостоятельно пользователем, подключение и реконфигурация любого элемента сети без согласования с системньTh1 администратором запрещено.

19. Подключение модемов и иных устройств на рабочих станциях для доступа в сеть запрещено. В исключительных случаях такие подключения осуществляет системный администратор с обязательным контролем этих рабочих станций.

Персональные компьютеры (рабочие станции).

20. Настройка операционной системы рабочих станций пользователей для корректной работы сети производится системным администратором.

21. Изменение конфигурации системы рабочих станций, установка новых программных продуктов и аппаратных средств, изменяющих настройки системы, самостоятельно или сторонними лицами без участия системного администратора запрещено.

22. Права и обязанности пользователей компьютерной сети регламентируются настоящим положением и должностными инструкциями.

23. Отключение пользователя сети от сетевых ресурсов производится с обязательным уведомлением данного пользователя.

24. При любых изменениях конфигурации подключения пользователя системным администратором производится обязательная проверка функционирования канала и доступа к ресурсам сети.

25. Несанкционированное расширение пользователями своих или чужих прав запрещено.

26. Запрещено изменять месторасположение рабочих станций без согласования.

27. В случае нарушения установленного порядка функционирования компьютерной сети виновные на основании рапорта системного администратора будут привлекаться к административной и материальной ответственности.

Права и обязанности пользователей локальной сети

28. Обязанности Пользователей сети:

– не предпринимать попыток нанесения ущерба (действием или бездействием) техническим и информационным ресурсам сети, а также исключить возможность неосторожного причинения вреда;

– использовать доступ к локальным и глобальным сетям только в профессиональных и служебных целях;

– пользователь локальной сети может входить в сеть только под своим именем и паролем, определяемыми в ходе регистрации. Запрещена передача сторонним лицам каких-либо сведений о настройке элементов сети (имена пользователей, пароли и т.д.).

– не использовать информационные и технические ресурсы сети в коммерческих целях и для явной или скрытой рекламы услуг, продукции и товаров любых организаций и физических лиц;

– не предпринимать попыток нанесения ущерба и попыток несанкционированного доступа к информационным и вычислительным ресурсам локальных и глобальных сетей, в том числе, не пытаться бесплатно или за чужой счет получить платную информацию;

– перед использованием или открытием файлов, полученных из глобальных или локальных сетей, или из других источников, проверять их на наличие вирусов;

– не использовать доступ к сети для распространения и тиражирования информации, распространение которой преследуется по закону, заведомо ложной информации и информации, порочащей организации и физические лица, а также служебной информации без соответствующего разрешения руководства образовательного учреждения;

– не распространять ни в какой форме (в том числе, в электронном или печатном виде) информацию, приравненную к служебной информации, полученную из информационных ресурсов образовательного учреждения;

– установить антивирусную программу из предложенных администратором сети, своевременно устанавливать обновления системы;

– соблюдать настройки сети;

– уважать права других пользователей на конфиденциальность и право на пользование общими ресурсами.

29. Пользователи локальной сети имеют право на:

– доступ к информационным ресурсам локальных и глобальных сетей;

– размещение информации пользователя среди информационных ресурсов локальной сети;

– пользователь сети имеет право обращаться к платной информации с разрешения руководителя образовательного учреждения. В этом случае пользователи оплачивают получаемые ими услуги самостоятельно.

Приложение 4
к приказу от 27.06.2023 г. № 73

Правила
работы с электронной почтой МАОУ «Гимназия № 41»

1. Политика использования электронной почты является важнейшим элементом политики информационной безопасности МАОУ «Гимназия № 41» и неотделима от нее.
2. Электронная почта является собственностью МАОУ «Гимназия № 41» и может быть использована только в служебных целях. Использование электронной почты МАОУ «Гимназия № 41» в других целях категорически запрещено.
3. Содержимое электронного почтового ящика МАОУ «Гимназия № 41» может быть проверено без предварительного уведомления по требованию директора МАОУ «Гимназия № 41» или его заместителей.
4. При работе с корпоративной системой электронной почты сотрудникам МАОУ «Гимназия № 41» запрещается:

– использовать адрес корпоративной почты для оформления подписок, без предварительного согласования с администрацией МАОУ «Гимназия № 41»;

– публиковать свой адрес, либо адреса других сотрудников МАОУ «Гимназия № 41» на общедоступных Интернет ресурсах (форумы, конференции и т.п.);

– отправлять сообщения с вложенными файлами общий объем которых превышает 5 Мегабайт;

– открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен; осуществлятьмассовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия. Данные действия квалифицируются как СПАМ и являются незаконными;

– осуществлять массовую рассылку почтовых сообщений рекламного характера без предварительного согласования с администрацией МАОУ «Гимназия № 41»;

– рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;

– распространять защищаемые авторскими правами материалы, затрагивающие какой- либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны; распространять информацию, содержание и направленность которой запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию,оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д. распространять информацию ограниченного доступа;

– предоставлять, кому быто ни было пароль доступа к почтовому ящику МАОУ «Гимназия № 41».

Приложение 5
к приказу от 27.06.2023 г. № 73

Положение об осуществлении антивирусной защиты в МАОУ «Гимназия № 41»

Общие положения

1. В Муниципальном автономном общеобразовательном учреждении «Гимназия № 41» (далее - МАОУ «Гимназия № 41») руководителем должно быть назначено лицо, ответственное за антивирусную защиту. В противном случае вся ответственность за обеспечение антивирусной защиты ложится на руководителя МАОУ «Гимназия № 41».
2. В МАОУ «Гимназия № 41» может использоваться только лицензионное антивирусное программное обеспечение. На период отсутствия лицензионного программного обеспечения МАОУ «Гимназия № 41» может использовать известные бесплатные антивирусные пакеты, своевременно обновляющие через Интернет.
3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).
4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

Требования к проведению мероприятий по антивирусной защите

5. В начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и серверов.
6. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю.
7. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на серверах и персональных компьютерах муниципального общеобразовательного учреждения.
8. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).
9. При отправке и получении электронной почты пользователь обязан проверить электронные письма на наличие вирусов.
10. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:

– Приостановить работу.

– Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в МАОУ «Гимназия № 41».

– Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использовании.

– Провести лечение или уничтожение зараженных файлов.

Ответственность

11. Ответственность за организацию антивирусной защиты возлагается на руководителя МАОУ «Гимназия № 41» или лицо, им назначенное.

12. Ответственность за проведение мероприятий антивирусного контроля в МАОУ «Гимназия № 41» и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение антивирусной защиты.

13. Периодический контроль за состоянием антивирусной защиты в МАОУ «Гимназия № 41» осуществляется руководителем.

Приложение 6
к приказу от 27.06.2023 г. № 73

Инструкция по организации антивирусной защиты в МАОУ «Гимназия № 41»

Общие положения

1. В МАОУ «Гимназия № 41» директор назначает лицо ответственное за антивирусную защиту.
2. В МАОУ «Гимназия № 41» используется лицензионное антивирусное программное обеспечение.
3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).
4. Файлы, помещаемые в электронный архив, в обязательном порядке должны проходить антивирусный контроль.
5. Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется на отсутствие вирусов.
6. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения регистрируется в специальном журнале за подписью лица, ответственного за антивирусную защиту.

Требования к проведению мероприятий по антивирусной защите

7. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезапуске) в автоматическом режиме должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех дисков и файлов персонального компьютера.
8. Периодические проверки электронных архивов проводятся не реже одного раза в неделю.
9. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера выполняется:

– Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), выполняется антивирусная проверка: на серверах и персональных компьютерах образовательного учреждения. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения регистрируется в специальном журнале за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего.

– При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

10. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

– приостановить работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в учреждении;

– совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

– провести лечение или уничтожение зараженных файлов;

– в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, ответственный за антивирусную защиту направляет зараженный вирусом файл на гибком магнитном диске в организацию, с которой заключен договор на антивирусную поддержку для дальнейшего исследования;

Ответственность

11. Ответственность за организацию антивирусной защиты возлагается на директора учреждения или лицо им назначенное.

12. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение антивирусной защиты.

13. Периодический контроль за состоянием антивирусной защиты в учреждении осуществляется заместителем директора по мониторингу и информатизации.

Приложение 7
к приказу от 27.06.2023 г. № 73

Должностная инструкция
ответственного за информационную безопасность

Общие положения

1. Настоящая должностная инструкция разработана и утверждена в соответствии с положениями Трудового кодекса Российской Федерации и иных нормативных актов, регулирующих трудовые правоотношения в Российской Федерации.
2. Настоящее инструкция определяет задачи, функции, обязанности, ответственность и права ответственного за работу в сети Интернет и за информационную безопасность (далее «ответственный за информационную безопасность») в Муниципальном автономном общеобразовательном учреждении «Гимназия № 41» (МАОУ «Гимназия № 41», далее- Гимназия).
3. Ответственный за информационную безопасность относится к категории специалистов и назначается приказом директора образовательного учреждения.
4. Ответственный за информационную безопасность подчиняется директору Гимназии.
5. Ответственный за информационную безопасность в пределах своих функциональных обязанностей обеспечивает безопасность информации, получаемой из сети Интернет и хранимой при помощи средств вычислительной техники в Гимназии.
6. Ответственный за информационную безопасность в своей работе руководствуется:

– законодательными и нормативными документами по вопросам обеспечения защиты информации;
– правилами техники безопасности и противопожарной защиты; методическими материалами, касающимися соответствующих вопросов; Уставом Гимназии;
– правилами внутреннего трудового распорядка;
– приказами и распоряжениями директора Гимназии (непосредственного руководителя);
– настоящей должностной инструкцией.

7. Ответственный за информационную безопасность должен знать:

– законодательные акты, нормативные и методические материалы по вопросам, связанным с обеспечением защиты информации;
– оснащенность вычислительных центров техническими средствами, перспективы их развития и модернизации;
– систему организации комплексной защиты информации, действующей в отрасли: методы и средства контроля охраняемых сведений, выявления каналов утечки информации, организацию технической разведки;
– методы планирования и организации проведения работ по защите информации и обеспечению государственной тайны;
– технические средства контроля и защиты информации, перспективы и направления их совершенствования;
– методы проведения специальных исследований и проверок, работ по защите технических средств передачи, обработки, отображения и хранения информации; порядок

пользования реферативными и справочно-информационными изданиями, а также другими источниками научно-технической информации;

– достижения науки и техники в стране и за рубежом в области технической разведки и защиты информации;

– методы и средства выполнения расчетов и вычислительных работ; основы экономики, организации производства, труда и управления; основы трудового законодательства Российской Федерации;

– правила и нормы охраны труда, техники безопасности, производственной санитарии и противопожарной защиты и др.

8. Во время отсутствия специалиста по защите информации (командировка, отпуск, болезнь и пр.) его обязанности исполняет лицо, назначенное в установленном порядке. Данное лицо приобретает соответствующие права и несет ответственность за надлежащее выполнение возложенных на него обязанностей.

Функции

9. Обеспечение комплексной защиты информации, соблюдения государственной тайны.

10. Участие в обследовании, аттестации и категорировании объектов защиты.

11. Разработка организационно-распорядительных документов, регламентирующих работу по защите информации.

12. Определение потребности в технических средствах защиты и контроля.

13. Проверка выполнения требований нормативных документов по защите информации.

Должностные обязанности

14. Ответственный за информационную безопасность:

– планирует использование ресурсов сети Интернет в Гимназии на основании заявок преподавателей и других работников образовательного учреждения;

– разрабатывает, согласует с педагогическим коллективом, представляет на педагогическом совете Гимназии регламент использования сети Интернет в образовательном учреждении, включая регламент определения доступа к ресурсам сети Интернет;

– обеспечивает функционирование и поддерживает работоспособность средств и систем защиты информации в пределах, возложенных на него обязанностей;

– организует получение сотрудниками Гимназии электронных адресов и паролей для работы в сети Интернет и информационной среде образовательного учреждения;

– организует контроль за использованием сети Интернет в образовательном учреждении;

– организует контроль за работой оборудования и программных средств, обеспечивающих использование сети Интернет и ограничение доступа;

– разрабатывает и готовит к утверждению проекты нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов по информационной безопасности;

– проводит обучение персонала и пользователей вычислительной техники правилам безопасной обработки информации и правилам работы со средствами защиты информации;

– устанавливает по согласованию с директором Гимназии критерии доступа пользователей;

– проводит текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации;

– обеспечивает контроль целостности эксплуатируемого на средствах вычислительной техники программного обеспечения с целью выявления несанкционированных изменений в нём;

– организует контроль за санкционированным изменением ПО, заменой и ремонтом средств вычислительной техники;

– немедленно докладывает директору о выявленных нарушениях и несанкционированных действиях пользователей и сотрудников, а также принимает необходимые меры по устранению нарушений;

– организовывает разработку и своевременное представление предложений для включения в соответствующие разделы перспективных и текущих планов работ и программ, мер по контролю и защите информации;

– осуществляет проверку выполнения требований межотраслевых и отраслевых: нормативных документов по защите информации;

– систематически повышает свою профессиональную квалификацию, общепедагогическую и предметную компетентность, включая ИКТ-компетентность, компетентность в использовании возможностей Интернета в учебном процессе;

– обеспечивает информирование организаций, отвечающих за работу технических и программных средств, об ошибках в работе оборудования и программного обеспечения;

– соблюдает правила и нормы охраны труда, техники безопасности и противопожарной защиты, правила использования сети Интернет.

15. Должен знать:

– дидактические возможности использования ресурсов сети Интернет;

– правила безопасного использования сети Интернет.

Права

16. Ответственный за информационную безопасность имеет право:

– Знакомиться с проектами решений руководства Гимназии, касающимися его деятельности.

– Определять ресурсы сети Интернет, используемые в учебном процессе на основе запросов преподавателей и по согласованию с руководителем образовательного учреждения.

– Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с обязанностями, предусмотренными настоящей инструкцией.

– Получать от руководителей структурных подразделений, специалистов информацию и документы, необходимые для выполнения своих должностных обязанностей.

– Привлекать преподавателей и специалистов Гимназии для решения возложенных на него обязанностей с разрешения руководителя Гимназии.

– Требовать от сотрудников и пользователей компьютерной техники безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения и электронных платежей.

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

– Требовать от руководства Гимназии оказания содействия в исполнении своих должностных обязанностей и прав.

Ответственность

17. Ответственный за информационную безопасность несет ответственность:

– За выполнение правил использования Интернета и ограничения доступа, установленного в образовательном учреждении;

– За качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определенными настоящей инструкцией.

– За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, в пределах, определенных трудовым законодательством Российской Федерации.

– За совершенные в процессе осуществления своей деятельности правонарушения - в пределах, определенных административным, уголовным и гражданским законодательством Российской Федерации.

– За причинение материального ущерба - в пределах, определенных трудовым, уголовным и гражданским законодательством Российской Федерации

Приложение 8
к приказу от 27.06.2023 г. № 73

Классификатор информации, не имеющей отношения к образовательному процессу

№№	Тематическая категория	Содержание
1	Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения	• Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды; • информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение
2	Злоупотребление свободой СМИ — экстремизм	Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы
3	Злоупотребление свободой СМИ — наркотические средства	Сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров
4	Злоупотребление свободой СМИ — информация с ограниченным доступом	Сведения о специальных средствах, технических приемах и тактике проведения контртеррористических операций
5	Злоупотребление свободой СМИ — скрытое воздействие	Информация, содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающая вредное влияние на их здоровье
6	Экстремистские материалы или экстремистская деятельность (экстремизм)	А) Экстремистские материалы, то есть предназначенные для обнародования документы или информация, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии; публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы;

№№	Тематическая категория	Содержание
		Б) экстремистская деятельность (экстремизм) включает деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков: • насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации; • подрыв безопасности Российской Федерации, захват или присвоение властных полномочий, создание незаконных вооруженных формирований; • осуществление террористической деятельности либо публичное оправдание терроризма; • возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию; • унижение национального достоинства; • осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической, расовой, национальной или религиозной ненависти либо вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы; • пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности; • воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, сопровождаемое насилием или угрозой его применения; • публичная клевета в отношении лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, при исполнении им своих должностных обязанностей или в связи с их исполнением, сопровождаемая обвинением указанного лица в совершении деяний, указанных в настоящей статье, при условии, что факт клеветы установлен в судебном порядке;

№№	Тематическая категория	Содержание
		• применение насилия в отношении представителя государственной власти либо угроза применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей; • посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность; • нарушение прав и свобод человека и гражданина, причинение вреда здоровью и имуществу граждан в связи с их убеждениями, расовой или национальной принадлежностью, вероисповеданием, социальной принадлежностью или социальным происхождением
7	Вредоносные программы	Программы для ЭВМ, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети
8	Преступления	• Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию); • оскорбление (унижение чести и достоинства другого лица, выраженное в неприличной форме); • публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма; • склонение к потреблению наркотических средств и психотропных веществ; • незаконное распространение или рекламирование порнографических материалов; • публичные призывы к осуществлению экстремистской деятельности; • информация, направленная на пропаганду национальной, классовой, социальной нетерпимости, а также социального, расового, национального и религиозного неравенства; • публичные призывы к развязыванию агрессивной войны
9	Ненадлежащая реклама	Информация, содержащая рекламу алкогольной продукции и табачных изделий

№№	Тематическая категория	Содержание
10	Информация с ограниченным доступом	Информация, составляющая государственную, коммерческую, служебную или иную охраняемую законом тайну

Приводимый далее перечень категорий Классификатора информации, не имеющей отношения к образовательному процессу, может быть дополнен, расширен или иным образом изменен в установленном порядке, в том числе с учетом специфики образовательного учреждения, социокультурных особенностей региона и иных обстоятельств.

№№	Тематическая категория	Содержание
1	Алкоголь	Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию
2	Баннеры и рекламные программы	Баннерные сети, всплывающая реклама, рекламные программы
3	Вождение и автомобили (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация об автомобилях и других транспортных средствах, вождении, автозапчастях, автомобильных журналах, техническом обслуживании, аксессуарах к автомобилям
4	Досуг и развлечения (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация: • фотоальбомы и фотоконкурсы; • рейтинги открыток, гороскопов, сонников; • гадания, магия и астрология; • ТВ-программы; • прогнозы погоды; • тесты, конкурсы онлайн; • туризм, путешествия; • тосты, поздравления; • кроссворды, сканворды, ответы к ним; • фантастика; • кулинария, рецепты, диеты; • мода, одежда, обувь, модные аксессуары, показы мод; • тексты песен, кино, киноактеры, расписания концертов, спектаклей, кинофильмов, заказ билетов в театры, кино и т.п.; • о дачах, участках, огородах, садах, цветоводстве, животных, питомцах, уходе за ними;

№№	Тематическая категория	Содержание
		• о рукоделии, студенческой жизни, музыке и музыкальных направлениях, группах, увлечениях, хобби, коллекционировании; • о службах знакомств, размещении объявлений онлайн; • анекдоты, «приколы», слухи; • о сайтах и журналах для женщин и для мужчин; • желтая пресса, онлайн-ТВ, онлайн-радио; • о знаменитостях; • о косметике, парфюмерии, прическах, ювелирных украшениях.
5	Здоровье и медицина (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация о шейпинге, фигуре, похудении, медицине, медицинских учреждениях, лекарствах, оборудовании, а также иные материалы на тему «Здоровье и медицина», которые, являясь академическими, по сути, могут быть также отнесены к другим категориям (порнография, трупы и т.п.)
6	Компьютерные игры (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющие отношения к образовательному процессу компьютерные онлайновые и оффлайновые игры, советы для игроков и ключи для прохождения игр, игровые форумы и чаты
7	Корпоративные сайты, интернет-представительства негосударственных учреждений (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, сайты коммерческих фирм, компаний, предприятий, организаций
8	Личная и немодерируемая информация	Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники, блоги
9	Отправка SMS с использованием интернет-ресурсов	Сайты, предлагающие услуги по отправке SMS-сообщений
10	Модерируемые доски объявлений (ресурсы данной категории, не	Содержащие информацию, не имеющую отношения к образовательному процессу, модерируемые доски сообщений/объявлений, а также модерируемые чаты

№№	Тематическая категория	Содержание
	имеющие отношения к образовательному процессу)	
11	Нелегальная помощь школьникам и студентам	Банки готовых рефератов, эссе, дипломных работ и пр.
12	Неприличный и грубый юмор	Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека
13	Нижнее белье, купальники	Сайты, на которых рекламируется и изображается нижнее белье и купальники
14	Обеспечение анонимности пользователя, обход контентных фильтров	Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам; Peer-to-Peer программы, сервисы бесплатных прокси-серверов, сервисы, дающие пользователю анонимность
15	Онлайн-казино и тотализаторы	Электронные казино, тотализаторы, игры на деньги, конкурсы и пр.
16	Платные сайты	Сайты, на которых вывешено объявление о платности посещения веб-страниц
17	Поиск работы, резюме, вакансии (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-представительства кадровых агентств, банки вакансий и резюме
18	Поисковые системы (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-каталоги, системы поиска и навигации в Интернете
19	Религии и атеизм (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Сайты, содержащие, не имеющую отношения к образовательному процессу, информацию религиозной и антирелигиозной направленности.
20	Системы поиска изображений	Системы для поиска изображений в Интернете по ключевому слову или словосочетанию
21	СМИ (ресурсы данной категории, не имеющие отношения к образовательному процессу)	СМИ, содержащие новостные ресурсы и сайты СМИ (радио, телевидения, печати), не имеющие отношения к образовательному процессу.

№№	Тематическая категория	Содержание
22	Табак, реклама табака, пропаганда потребления табака	Сайты, пропагандирующие потребление табака; реклама табака и изделий из него
23	Торговля и реклама (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие, не имеющие отношения к образовательному процессу, сайты следующих категорий: аукционы, распродажи онлайн, интернет-магазины, каталоги товаров и цен, электронная коммерция, модели мобильных телефонов, юридические услуги, полиграфия, типографии и их услуги, таможенные услуги, охранные услуги, иммиграционные услуги, услуги по переводу текста на иностранные языки, канцелярские товары, налоги, аудит, консалтинг, деловая литература, дом, ремонт, строительство, недвижимость, аренда недвижимости, покупка недвижимости, продажа услуг мобильной связи (например, картинки и мелодии для сотовых телефонов), заработок в Интернете, е-бизнес
24	Убийства, насилие	Сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.
25	Чаты (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющие отношения к образовательному процессу сайты для анонимного общения в режиме онлайн.