Комитет образования администрации муниципального образования
Сосновоборский городской округ Ленинградской области
(Комитет образования Сосновоборского городского округа)

РАСПОРЯЖЕНИЕ

18.08.2014 **№ 108-р**

Об организации доступа образовательных организаций к сети Интернет, об организационных мерах, обеспечивающих исключение доступа обучающихся образовательных организаций к ресурсам сети Интернет, содержащим информацию, причиняющую вред здоровью и (или) развитию детей

Во исполнение требований Федерального закона от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и (или) развитию" (с изменениями и дополнениями), в целях исключения доступа обучающихся образовательных организаций (далее - ОО) к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания, в соответствии с Федеральным законом "Об образовании в Российской Федерации" от 29 декабря 2012г. № 273-ФЗ, методическими рекомендациями по ограничению в ОО доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (письмо Минобрнауки РФ от 28.04.2014 г. № ДЛ-115/03), методическими и справочными материалами для реализации комплексных мер по внедрению и использованию программно-технических средств, обеспечивающих исключение доступа обучающихся образовательных учреждений к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания (М.: ООО «МегаВерсия», 2006), письмом Минобразования России от 11.05.2011 № АФ-12/07 вн "Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Минобрнауки РФ", письмом Комитета образования от 19.05.2014 № 06-05-02-3115/14-0 "О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет и усилении контроля за организацией работы образовательных организаций с ресурсами сети Интернет", письмом комитета общего и профессионального образования Ленинградской области от 25.06.2014 № 19-3560/14-0-0 "Об организационных мерах, обеспечивающих исключение доступа обучающихся образовательных организаций к ресурсам сети Интернет, содержащим информацию, причиняющую вред здоровью и (или) развитию детей"

1. Утвердить минимальный перечень типовых (примерных) документов по организации доступа ОО к сети Интернет и обеспечению исключения доступа обучающихся ОО к ресурсам сети Интернет, содержащим информацию, причиняющую вред здоровью и (или) развитию детей:

1.1. Положение о Совете образовательной организации по вопросам регламентации доступа к информации в сети Интернет (приложение 1).

1.2. Правила использования сети Интернет в образовательной организации (приложение 2).

1.3. Регламент работы с электронной почтой (приложение 3).

1.4. Регламент организации антивирусной защиты (приложение 4).

1.5. Инструкция пользователя по компьютерной безопасности при работе в сети Интернет (приложение 5).

1.6. Инструкция для сотрудников образовательной организации о порядке действий при осуществлении контроля использования обучающимися сети Интернет (приложение 6).

1.7. Должностная инструкция отдельных работников образовательной организации с изменениями по использованию сети Интернет работником (приложение 7 - Рекомендации для внесения изменений в должностные инструкции отдельных работников образовательных организаций по использованию сети Интернет работником).

1.8. Классификаторы информации, причиняющей вред здоровью и (или) развитию детей (приложение 8):

- ✓классификатор информации, распространение которой запрещено в соответствии с законодательством Российской Федерации;
- ✓классификатор информации, запрещенной для распространения среди детей;
- ✓классификатор информации, распространение которой среди детей определенных возрастных категорий ограничено;
- ✓классификатор информации, не соответствующей задачам образования.

1.9. Форма журнала контроля за контентной фильтрацией (приложение 9);

1.10. Форма журнала проверок антивирусной защиты (приложение 10);

2. Утвердить примерную инструкцию по осуществлению самопроверки (мониторинга) эффективности работы системы контентной фильтрации (далее - СКФ) в ОО (приложение 11).

3. Руководителям всех типов ОО:

3.1. взять под личный контроль обеспечение эффективного и безопасного доступа к сети Интернет обучающихся ОО;

3.2. усилить контроль по организации мероприятий по обеспечению исключения доступа обучающихся ОО к ресурсам сети Интернет, содержащим информацию, причиняющую вред здоровью и (или) развитию детей;

3.3. назначить ответственного в ОО за контроль СКФ доступа к сети Интернет;

3.4. обеспечить установку контент-фильтров на каждом компьютере, включая административных работников;

3.5. провести в срок до 01.09.2014г. работу в ОО по приведению локальных правовых актов, регламентирующих доступ к сети Интернет, на основе утвержденных типовых документов (п.1.) в соответствии с действующим законодательством;

3.6. предоставить в срок до 03.09.2014г. в Комитет образования отчет о наличии локальных правовых актов и прочих документов, регламентирующих доступ в сеть Интернет, на бумажном носителе и в электронном виде по адресу kip@meria.sbor.ru Кириланд Ирине Павловне (форма отчета - приложение 12);

3.7. сформировать и утвердить персональный состав Совета ОО по вопросам регламентации доступа к информации в сети Интернет;

3.8. организовать проведение образовательных и консультационных мероприятий с родителями обучающихся с целью объяснения правил, рисков предоставления детям средств связи с выходом в сеть Интернет, проведение уроков по интернет-безопасности;

3.9. внести отдельное положение в договор об оказании образовательных услуг, предусматривающее запрет использования личных средств связи с выходом в сеть «Интернет» или согласие родителей о снятии ответственности с руководителя ОО в случае предоставления своему ребенку данного устройства при посещении ОО;

3.10. осуществлять по разработанной инструкции (п.2) ежеквартальные мониторинги эффективности использования СКФ в ОО (тестирование на каждом компьютере, имеющем выход в сеть Интернет, эффективности настройки программных средств, осуществляющих контентную фильтрацию) и предоставлять не позднее 01 числа месяца, следующего за отчетным периодом, в Комитет образования отчет о результатах мониторинга и акт (или протокол) проверки на бумажном носителе и в электронном виде по адресу kip@meria.sbor.ru Кириланд Ирине Павловне (форма мониторинга - приложение 13);

4. Главному специалисту Комитета образования Кириланд И.П.:

4.1. усилить контроль по организации мероприятий по обеспечению исключения доступа обучающихся ОО к ресурсам сети Интернет, содержащим информацию, причиняющую вред здоровью и (или) развитию детей;

4.2. предоставить в срок до 05.09.2014г. в комитет общего и профессионального образования Ленинградской области отчет о наличии нормативной базы в ОО, регламентирующей доступ в сеть Интернет;

4.3. осуществлять ежеквартальный мониторинг наличия и качества функционирования СКФ в ОО и предоставлять не позднее 3 числа месяца, следующего за отчетным периодом, начиная с 3 квартала 2014 года, в комитет общего и профессионального образования Ленинградской области отчет о результатах мониторинга эффективности использования СКФ в ОО.

5. Контроль за выполнением распоряжения оставляю за собой.

Председатель
Комитета образования М.Г. Мехоношина

исп. Кириланд И.П.,
т.2-99-73

С распоряжением ознакомлены:

Рассылка: все ОО (ООО, ОДОД, ДОО)

Приложение 1 к распоряжению КО
от 18.08.2014 № 108-р

Примерное положение о Совете образовательной организации по вопросам регламентации доступа к информации в сети Интернет

1. В соответствии с настоящим Положением о Совете образовательной организации (далее –ОО) по вопросам регламентации доступа к информации в Интернете (далее – Совет) целью создания Совета является принятие мер для исключения доступа обучающихся к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания обучающихся.

2. Совет осуществляет непосредственное определение политики доступа в Интернет.

3. Совет создается из представителей педагогического коллектива, профсоюзной организации (если таковая имеется), родительского комитета и ученического самоуправления в согласованном указанными лицами порядке.

4. Очередные Собрания Совета проходят с периодичностью, установленной Советом.

5. Совет:

- принимает решения о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет, содержащим информацию, несовместимую с задачами образовательного процесса с учетом социокультурных особенностей конкретного региона, с учетом мнения членов Совета, а также иных заинтересованных лиц, представивших свои предложения в Совет;

- определяет характер и объем информации, публикуемой на Интернет-ресурсах ОО;

- направляет руководителю ОО рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за непосредственный контроль безопасности работы обучающихся в сети Интернет и соответствия ее целям и задачам образовательного процесса.

6. Во время занятий контроль за использованием обучающимися сети Интернет осуществляет преподаватель. Во время использования сети Интернет для свободной работы обучающихся контроль за использованием сети Интернет осуществляет лицо, уполномоченное Советом (далее – Уполномоченное лицо).

7. Уполномоченное лицо:

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

- способствует осуществлению контроля за объемом трафика ОО в сети Интернет;

- наблюдает за использованием компьютеров и сети Интернет обучающимися;

- запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения обучающимся порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;

- не допускает обучающегося к работе в Интернете в предусмотренных настоящими Правилами случаях;

- принимает необходимые меры для пресечения дальнейших попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования.

8. Принятие решений о политике доступа к ресурсам/группам ресурсов сети Интернет осуществляется Советом самостоятельно либо с привлечением внешних экспертов, в качестве которых могут привлекаться:

- преподаватели ОО и других ОО;

- лица, имеющие специальные знания либо опыт работы в соответствующих областях;

- представители органов управления образованием.

9. При принятии решения Совет и эксперты должны руководствоваться:

- законодательством Российской Федерации;

- специальными познаниями, в том числе полученными в результате профессиональной деятельности по рассматриваемой тематике;

- интересами обучающихся, целями образовательного процесса;

- рекомендациями профильных органов и организаций в сфере классификации ресурсов сети Интернет.

10. Отнесение определенных категорий и/или ресурсов в соответствующие группы, доступ к которым регулируется техническим средствами и программным обеспечением контекстного технического ограничения доступа к информации, осуществляется на основании решений Совета лицом, уполномоченным руководителем ОО по представлению Совета.

11. Категории ресурсов, в соответствии с которыми определяется политика использования сети Интернет в ОО и доступ к которым регулируется техническими средствами и программным обеспечением контекстного технического ограничения доступа к информации, определяются в установленном порядке.

Приложение 2 к распоряжению КО
от 18.08.2014 № 108-р

Типовые правила использования сети Интернет в образовательной организации

(или можно разработать регламент организации доступа к сети Интернет)

Общие положения

1.1. Настоящие Правила регулируют условия и порядок использования сети Интернет через ресурсы образовательной организации (далее - ОО) обучающимися, преподавателями и сотрудниками ОО.

1.2. Настоящие Правила имеют статус локального нормативного акта ОО. Если нормами действующего законодательства Российской Федерации предусмотрены иные требования, чем настоящими Правилами, применяются нормы действующего законодательства Российской Федерации.

1.3. Использование сети Интернет в ОО подчинено следующим принципам:

- соответствия образовательным целям;
- способствования гармоничному формированию и развитию личности;
- уважения закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернета;
- приобретения новых навыков и знаний;
- расширения применяемого спектра учебных и наглядных пособий;
- социализации личности, введения в информационное общество.

Организация и политика использования сети Интернет в ОО

2.1. Использование сети Интернет в ОО возможно исключительно при условии ознакомления и согласия лица, пользующегося сетью Интернет в ОО, с настоящими Правилами.

Ознакомление и согласие удостоверяется подписью лица в Листе ознакомления и согласия с Правилами. Ознакомление и согласие несовершеннолетнего удостоверяется, помимо его подписи, также подписью его родителя или иного законного представителя.

2.2. Руководитель ОО является ответственным за обеспечение эффективного и безопасного доступа к сети Интернет в ОО, а также за внедрение соответствующих технических, правовых и др. механизмов в ОО.

2.3. Непосредственное определение политики доступа в Интернет осуществляет Совет ОО по вопросам регламентации доступа к информации в сети Интернет (далее – Совет), состоящий из представителей педагогического коллектива, сотрудников ОО, профсоюзной организации (если таковая имеется), родительского комитета и ученического самоуправления.

Очередные Собрания Совета проходят с периодичностью, установленной Советом.

Совет:

- принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет, содержащим информацию, запрещенную законодательством Российской Федерации и/или несовместимую с задачами образовательного процесса с учетом социокультурных особенностей конкретного региона;
- определяет характер и объем информации, публикуемой на Интернет-ресурсах ОО;
- дает руководителю ОО рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за непосредственный контроль безопасности работы в сети Интернет и соответствия ее целям и задачам образовательного процесса.

2.4. Во время занятий контроль за использованием обучающимися сети Интернет в соответствии с настоящим Правилами осуществляет преподаватель, ведущий занятие.

Преподаватель:

- наблюдает за использованием компьютера и сети Интернет обучающимися;

- запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения обучающимся настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в ОО;

- принимает предусмотренные настоящими Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования.

Во время использования сети Интернет для свободной работы контроль за использованием сети Интернет осуществляет лицо, уполномоченное на то Советом (далее – Уполномоченное лицо).

Уполномоченное лицо:

- определяет время и место для свободной работы в сети Интернет обучающихся, преподавателей и сотрудников ОО с учетом использования соответствующих технических мощностей ОО в образовательном процессе, а также длительность сеанса работы одного человека;

- контролирует объем трафика ОО в сети Интернет;

- наблюдать за использованием компьютера и сети Интернет обучающимися;

- запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения обучающимся настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в ОО;

- не допускает обучающегося к работе в Интернете в предусмотренных настоящими Правилами случаях;

- принимает предусмотренные настоящими Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования.

2.5. При использовании сети Интернет в ОО осуществляется доступ только на ресурсы, содержание которых не противоречит законодательству Российской Федерации и не является несовместимым с целями и задачами образования и воспитания обучающихся.

В соответствии со ст. 6.17 Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ руководитель ОО несет ответственность за нарушение законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию.

В соответствии с п.15 ч.3 ст.28 Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации» к компетенции ОО относится создание необходимых условий для охраны и укрепления здоровья обучающихся и работников.

В соответствии со ст.11, ч. 1 ст. 14 Федерального закона № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» образовательные организации, предоставляя для детей компьютеры, имеющие выход в Интернет, во время образовательного процесса и вне учебного времени, обязаны применять определенные административные и организационные меры, технические и программно-аппаратные средства защиты детей от указанной информации и несут ответственность за доступ к информации, наносящей вред здоровью несовершеннолетнего.

2.6. Принятие решения о политике доступа к ресурсам/группам ресурсов сети Интернет принимается Советом самостоятельно либо с привлечением внешних экспертов, в качестве которых могут привлекаться:

- преподаватели ОО и других ОО;

- лица, имеющие специальные знания либо опыт работы в рассматриваемой области;

- представители органов управления образованием.

При принятии решения Совет, эксперты руководствуются:

- законодательством Российской Федерации;

- специальными познаниями, в том числе полученными в результате профессиональной деятельности по рассматриваемой тематике;

- интересами обучающихся, целями образовательного процесса;

- рекомендациями профильных органов и организаций в сфере классификации ресурсов сети Интернет.

2.7. Отнесение определенных категорий и/или ресурсов в соответствующие группы, доступ к которым регулируется техническим средствами и программным обеспечением

контекстного технического ограничения доступа к информации, осуществляется лицом, уполномоченным руководителем ОО по представлению Совета.

Категории ресурсов, в соответствии с которыми определяется политика использования сети Интернет в ОО и доступ к которым регулируется техническими средствами и программным обеспечением контекстного технического ограничения доступа к информации, определяются в установленном порядке.

2.8. Принципами размещения информации на Интернет-ресурсах ОО являются:

- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
- защита персональных данных обучающихся, преподавателей и сотрудников;
- достоверность и корректность информации.

Персональные данные об обучающихся (фамилия и имя, класс, возраст, фотография, место жительства, телефоны и иные контакты, иные сведения личного характера) могут размещаться на Интернет-ресурсах ОО (сайт ОО и ее подразделений) только с письменного согласия родителей или иных законных представителей обучающихся. Персональные данные преподавателей и сотрудников ОО размещаются на Интернет-ресурсах ОО только с письменного согласия преподавателя или сотрудника, чьи персональные данные размещаются.

В информационных сообщениях о мероприятиях на сайте ОО и ее подразделений без согласия лица или его законного представителя могут быть упомянуты только фамилия и имя обучающегося либо фамилия, имя и отчество преподавателя\сотрудника\родителя.

При истребовании такого согласия представитель ОО и (или) представитель Совета разъясняет лицу возможные риски и последствия опубликования персональных данных. ОО не несет ответственности в случае наступления таких последствий, если имелось письменное согласие лица (его представителя) на опубликование персональных данных.

Процедура использования сети Интернет

3.1. Использование сети Интернет в ОО осуществляется, как правило, в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области сети Интернет и компьютерной грамотности лицо может осуществлять доступ к ресурсам необразовательной направленности.

3.2. По разрешению Уполномоченного лица обучающиеся (с согласия родителей, законных представителей), преподаватели и сотрудники вправе:

- размещать собственную информацию в сети Интернет на Интернет-ресурсах ОО;
- иметь учетную запись электронной почты на Интернет-ресурсах ОО.

3.3. Обучающемуся запрещается:

- находиться на ресурсах, содержание и тематика которых является недопустимой для несовершеннолетних и/или нарушающей законодательство Российской Федерации (4 классификатора информации, причиняющей вред здоровью и (или) развитию детей);
- осуществлять загрузки файлов на компьютер ОО без разрешения уполномоченного лица;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.4. Уполномоченное лицо проверяет, является ли данный обучающийся допущенным до самостоятельной работы в сети Интернет.

3.5. При случайном обнаружении лицом, работающим в сети Интернет, ресурса, содержимое которого несовместимо с целями образовательного процесса, он обязан незамедлительно сообщить о таком ресурсе Уполномоченному лицу с указанием его Интернет-адреса (URL) и покинуть данный ресурс.

Уполномоченное лицо обязано:

- принять сообщение лица, работающего в сети Интернет;
- довести информацию до сведения Совета для оценки ресурса и принятия решения по политике доступа к нему в соответствии с п.2.3 настоящих Правил;
- направить информацию о некатегоризированном ресурсе оператору технических средств и программного обеспечения технического ограничения доступа к информации (в течение суток);

- если обнаруженный ресурс явно нарушает законодательство Российской Федерации – сообщить об обнаруженном ресурсе по специальной «горячей линии» для принятия мер в соответствии с законодательством Российской Федерации (в течение суток).

Передаваемая информация должна содержать:

- Интернет-адрес (URL) ресурса;
- Тематику ресурса, предположения о нарушении ресурсом законодательства Российской Федерации либо несовместимости с задачами образовательного процесса;
- Дату и время обнаружения;
- Информацию об установленных в ОО технических средствах технического ограничения доступа к информации.

Приложение 3 к распоряжению КО
от 18.08.2014 № 108-р

Примерный регламент работы с электронной почтой

Политика использования электронной почты является важнейшим элементом общекорпоративной политики информационной безопасности Городской информационной образовательной сети (ГИОС) и неотделима от нее. Электронная почта может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

1. Общие положения

1.1. Электронная почта в образовательной организации (далее – ОО) может использоваться только в функциональных и образовательных целях.
1.2. Для официальной переписки должны использоваться только ящики электронной почты из домена edu.sbor.net.
1.3. Настройку учетных записей почтовых служб на сервере производит ответственный инженер МАОУ ДОД ЦИТ по заявкам ОО.
1.4. Пользователи должны соблюдать правила и инструкции по работе с электронной почтой, этические нормы общения.

2. Порядок обработки, передачи и приема документов по электронной почте.

2.1. По электронной почте производится получение и отправка информации законодательного, нормативно-правового, учебного, учебно-методического характера.
2.2. ОО обеспечивает бесперебойное получение электронной почты не реже трех раз в день.
2.3. Передаваемые с помощью электронной почты официальные документы должны иметь исходящий регистрационный номер.
2.4. Все передаваемые учебно-методические и справочно-информационные материалы должны передаваться с сопроводительным письмом.
2.5. Перед отправлением сообщения необходимо проверять правописание и грамматику текста.
2.6. Все учебно-методические и справочно-информационные материалы передаются в виде прикрепленных файлов с сопроводительным письмом, краткая информация просто помещается в текст письма, а не прикрепляется отдельным файлом.
2.7. В строке «Тема:» четко указывается краткое содержание послания (заголовок).

3. Пользователям запрещено:

3.1. Участвовать в рассылке посланий, не связанных с образовательным процессом.
3.2. Пересылать по произвольным адресам не затребованную потребителями информацию (спам). В случае обнаружения рассылки спама электронные почтовые ящики будут блокированы до выявления причин и нарушителей.
3.3. Отправлять сообщения противозаконного или неэтичного содержания.
3.4. Использовать массовую рассылку почты, за исключением необходимых случаев.
3.5. Электронное послание не должно использовать для пересылки секретной и конфиденциальной информации, поскольку является эквивалентом почтовой открытки.
3.6. Публиковать свой адрес, либо адреса других сотрудников ОО на общедоступных Интернет ресурсах (форумы, конференции и т.п.).
3.7. 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.

Приложение 4 к распоряжению КО
от 18.08.2014 № 108-р

Регламент организации антивирусной защиты

1. Общие положения

1.1. В образовательной организации (далее – ОО) руководителем должно быть назначено лицо, ответственное за антивирусную защиту. В противном случае вся ответственность за обеспечение антивирусной защиты ложится на руководителя ОО.

1.2. В ОО может использоваться только лицензионное антивирусное программное обеспечение.

1.3. 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).

1.4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

1.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

2. Требования к проведению мероприятий по антивирусной защите

2.1. 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.

2.2. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю.

2.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

- после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка: на серверах и персональных компьютерах ОО. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться 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.).

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

- приостановить работу;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение (при невозможности лечения) зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, ответственный за антивирусную защиту обязан направить зараженный вирусом файл на гибком магнитном диске в организацию, с которой заключен договор на антивирусную поддержку для дальнейшего исследования.

3. Ответственность

3.1. Ответственность за организацию антивирусной защиты возлагается на руководителя ОО или лицо им назначенное.

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

3.3. Периодический контроль за состоянием антивирусной защиты в ОО осуществляется руководителем.

Приложение 5 к распоряжению КО
от 18.08.2014 № 108-р

Примерная инструкция пользователя по компьютерной безопасности при работе в сети Интернет

1. Установить последние обновления операционной системы Windows (http://windowsupdate.microsoft.com)
2. Включить режим автоматической загрузки обновлений. (Пуск->Настройка->панель управления->Автоматическое обновление->Автоматически загружать и устанавливать на компьютер рекомендуемые обновления).
3. Скачать с сайта www.microsoft.com программное обеспечение Windows Defender и установить на все компьютеры. Включить режим автоматической проверки. Включить режим проверки по расписанию каждый день.
4. Активировать встроенный брандмауэр Windows (Пуск->Настройка->панель управления->Брандмауэр Windows->Включить).
5. Установить антивирусное программное обеспечение на каждый компьютер. Включить режим автоматического сканирования файловой системы. Включить режим ежедневной автоматической проверки всей файловой системы при включении компьютера. Активировать функцию ежедневного автоматического обновления антивирусных баз.
6. Ежедневно проверять состояние антивирусного программного обеспечения, а именно
    a. Режим автоматической защиты должен быть включен постоянно
    b. Дата обновления антивирусных баз не должна отличаться более чем на несколько дней от текущей даты.
    c. Просматривать журналы ежедневных антивирусных проверок. Контролировать удаление вирусов при их появлении.
7. Не реже одного раза в месяц посещать сайт http://windowsupdate.microsoft.com и проверять установлены ли последние обновления операционной системы.
8. Быть крайне осторожным при работе с электронной почтой. Категорически запрещается открывать присоединенные к письмам, полученным от незнакомых лиц, файлы.
9. Контролировать посещение Интернет сайтов пользователями. Не допускать посещения т.н. «хакерских», порно и других сайтов с потенциально вредоносным содержанием.
10. В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними.
11. При появлении признаков нестандартной работы компьютера («тормозит», на экране появляются и исчезают окна, сообщения, изображения, самостоятельно запускаются программы и т.п.) немедленно отключить компьютер от Ethernet сети, загрузить компьютер с внешнего загрузочного диска (CD, DVD) и произвести полную антивирусную проверку всех дисков компьютера. При появлении аналогичных признаков после проделанной процедуры переустановить операционную систему с форматированием системного раздела диска.

Приложение 6 к распоряжению КО
от 18.08.2014 № 108-р

Типовая инструкция для сотрудников образовательной организации о порядке действий при осуществлении контроля использования обучающимися сети Интернет

1. Настоящая Инструкция устанавливает порядок действий при обнаружении сотрудниками образовательных организаций (далее – ОО) и экспертно-консультативных органов (советов):

- возможности доступа обучающихся к потенциально опасному контенту;
- вызванного техническими причинами отказа доступа к контенту, не представляющему опасности для обучающихся, доступ к которому не противоречит принятым нормативным актам на федеральном уровне, уровне субъекта Российской Федерации, муниципальном уровне, а также на уровне ОО.

2. Контроль за использованием обучающимися сети Интернет осуществляют:

- во время проведения занятий – преподаватель, проводящий занятие и (или) специально уполномоченное руководством ОО на осуществление такого контроля лицо;
- во время использования сети Интернет для свободной работы обучающихся - лицо, уполномоченное Советом ОО по вопросам регламентации доступа к информации в Интернете (далее – Совет) или руководителем ОО в установленном Советом порядке.

3. Лицо, осуществляющее контроль за использованием обучающимися сети Интернет:

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

- способствует осуществлению контроля за объемом трафика ОО в сети Интернет;

- наблюдает за использованием компьютеров и сети Интернет обучающимися;

- запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения обучающимся порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;

- не допускает обучающегося к работе в Интернете в предусмотренных Правилами использования сети Интернет случаях;

- принимает необходимые меры для пресечения дальнейших попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования.

4. При обнаружении информации, в отношении которой у лица, осуществляющего контроль за использованием обучающимися сети Интернет, возникают основания предполагать, что такая информация относится к числу запрещенной для распространения в соответствии с законодательством Российской Федерации или иному потенциально опасному для обучающихся контенту, ответственное лицо направляет соответствующую информацию руководителю ОО и в Совет, которые принимают необходимые решения.

5. При обнаружении вызванного техническими причинами отказа доступа к контенту, не представляющему опасности для обучающихся, доступ к которому не противоречит принятым нормативным актам на федеральном уровне, уровне субъекта Российской Федерации, муниципальном уровне, а также на уровне ОО.

Приложение 7 к распоряжению КО
от 18.08.2014 № 108-р

Рекомендации для внесения изменений в должностные инструкции отдельных работников образовательных организаций

В должностные инструкции работников образовательных организаций (далее – ОО) рекомендуется внести дополнительно следующие положения.

Преподаватель:

1. Общие положения

Должен знать:
- дидактические возможности использования ресурсов сети Интернет;
- правила безопасного использования сети Интернет.

2. Должностные обязанности:

- планирует использование ресурсов сети Интернет в учебном процессе с учетом специфики преподаваемого предмета;
- разрабатывает, согласует с методическим объединением, представляет на педагогическом совете ОО и размещает в информационном пространстве ОО календарно-тематическое планирование;
- ведет записи в регистрационном журнале доступа к сети (Приложение 4);
- использует разнообразные приемы, методы и средства обучения, в том числе возможности сети Интернет;
- систематически повышает свою профессиональную квалификацию, общепедагогическую и предметную компетентность, включая ИКТ-компетентность, компетентность в использовании возможностей Интернета в учебном процессе;
- соблюдает правила и нормы охраны труда, техники безопасности и противопожарной защиты, правила использования сети Интернет.

3. Права

Вправе определять ресурсы сети Интернет, используемые обучающимися в учебном процессе.

4. Ответственность

Несет ответственность за выполнение обучающимися правил доступа к ресурсам сети Интернет в ходе учебного процесса.

Сотрудник ОО, назначенный ответственным за работу Интернета и ограничение доступа:

Ответственный за работу Интернета и ограничение доступа назначается приказом руководителя ОО. В качестве ответственного за организацию доступа к сети Интернет может быть назначен заместитель руководителя ОО по учебно-воспитательной работе, заместитель руководителя ОО по информатизации, преподаватель информатики, другой сотрудник ОО.

1. Общие положения

Должен знать:
- дидактические возможности использования ресурсов сети Интернет;
- правила безопасного использования сети Интернет.

2. Должностные обязанности:

- планирует использование ресурсов сети Интернет в ОО на основании заявок преподавателей и других работников ОО;

- разрабатывает, согласует с педагогическим коллективом, представляет на Совете ОО регламент использования сети Интернет в ОО, включая регламент определения доступа к ресурсам сети Интернет;

- обеспечивает администрирование сети (компьютера);

- по решению Совета ОУ организует получение сотрудниками ОО электронных адресов и паролей для работы в сети Интернет и информационной среде ОО;

- организует контроль использования сети Интернет в ОО;

- ведет регистрационный журнал доступа к сети;

- организует контроль работы оборудования и программных средств, обеспечивающих использование сети Интернет и ограничение доступа;

- 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.

3. Права

Вправе определять ресурсы сети Интернет, используемые обучающимися в учебном процессе, в пределах рекомендуемого контента на основе запросов преподавателей.

4. Ответственность

Несет ответственность за выполнение правил использования Интернета и ограничения доступа, установленного в ОО.

Приложение 8 к распоряжению КО
от 18.08.2014 № 108-р

Классификаторы информации, причиняющей вред здоровью и (или) развитию детей

№ п/п	Наименование тематической категории	Содержание
а) классификатор информации, распространение которой запрещено в соответствии с законодательством Российской Федерации		
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, пропаганду 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 контртеррористической операции
5	Злоупотребление свободой СМИ / скрытое воздействие	Содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающих вредное влияние на их здоровье
6	Экстремистские материалы или экстремистская деятельность (экстремизм)	А) Экстремистские материалы, т.е. предназначенные для обнародования документы либо 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; Б) экстремистская деятельность (экстремизм) включает в себя 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; - пропаганду 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, соединенное с насилием или угрозой его применения; - публичную клевету 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, соединенную с обвинением указанного лица в совершении деяний, указанных в настоящей статье, при условии, что факт клеветы установлен в судебном порядке; - применение насилия в отношении представителя государственной власти либо на угрозу 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 неприлично 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 пропаганду социального, расового, национального и религиозного неравенства; - публичные призывы к развязыванию агрессивной войны.
9	Ненадлежащая реклама	Информация, содержащая рекламу алкогольной продукции и табачных изделий
10	Информация с ограниченным доступом	Информация, составляющая государственную, коммерческую, служебную или иную специально охраняемую законом тайну
б) классификатор информации, запрещенной для распространения среди детей		
1.	Побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описания и/или изображения способов причинения вреда своему здоровью, самоубийства; обсуждения таких способов и их последствий; мотивирующая на совершение таких действий
2.	Способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет») содержащая рекламу или объявления/предложения о продаже наркотических средств, психотропных и (или) одурманивающих веществ, табачных изделий, алкогольной и спиртосодержащей продукции, пива и напитков, изготавливаемых на его основе, участии в азартных игра, использовании или вовлечении в проституцию, бродяжничество или попрошайничество; содержащую обсуждение или организующую активность на данную тему

3.	Обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных Федеральным законом № 436-ФЗ	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, аудио и видеоматериалы актов насилия или жестокости, жертв насилия и жестокости, участников актов насилия и жестокости; обосновывающие или оправдывающие акты геноцида, военных преступлений, преступлений против человечности, террористических акций, массовых и серийных убийств; содержащие обсуждения участия в или планирование совершающихся или будущих актов насилия или жестокости
4.	Отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), призывающая к отказу от семьи и детей («чайлдфри»), страницы клубов для лиц нетрадиционной сексуальной ориентации, сообщества и ресурсы знакомств людей нетрадиционной сексуальной ориентации, содержащая описания, фотографии, рисунки, аудио и видеоматериалы, описывающие и изображающие нетрадиционные сексуальные отношения
5.	Оправдывающая противоправное поведение	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, аудио и видеоматериалы, содержащие призывы к противоправному поведению, одобрение противоправного поведения
6.	Содержащая нецензурную брань	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая нецензурную брань
7.	Содержащая информацию порнографического характера	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, аудио и видеоматериалы по данной теме
8.	О несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию,	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, аудио и видеоматериалы по данной теме

	позволяющую прямо или косвенно установить личность такого несовершеннолетнего	
в) классификатор информации, распространение которой среди детей определенных возрастных категорий ограничено		
1.	Представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, видеоматериалы по данной теме
2.	Вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, видеоматериалы по данной теме
3.	Представляемая в виде изображения или описания половых отношений между мужчиной и женщиной	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, видеоматериалы по данной теме
4.	Содержащая бранные слова и выражения, не относящиеся к нецензурной брани	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая указанные виды информации
г) классификатор информации, не соответствующей задачам образования.		
1.	Информация досугового и развлекательного характера, за исключением соответствующей задачам образования	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет») по следующим направлениям: рейтинги открыток, гороскопов, сонников; гадания, магия и астрология; тесты, конкурсы, организуемые в сети «Интернет», за исключением образовательных конкурсов, тестов (таких как тесты на знание иностранных языков и уровни полученных знаний) и олимпиад; тосты; службы знакомств; анекдоты, «приколы», слухи; специализированные сайты, распространяющие развлекательный контент для мобильных устройств (рингтоны, заставки, картинки, игры, рассылки и т.п.)
2.	Нетрадиционная медицина	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет») по направлениям нетрадиционной медицины, народных целителей, БАД
3.	Компьютерные игры, за исключением соответствующей задачам образования	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), по тематике компьютерных игр, не соответствующая задачам образования, такая как порталы браузерных игр, массовые многопользовательские онлайн ролевые игры (MMORPG), массовые

		многопользовательские игры, основанные на имитации боевых или противоправных действий, советы для игроков и ключи для установки и прохождения игр, игровые форумы и чаты
4.	Ресурсы, базирующиеся либо ориентированные на обеспечении анонимности распространителей и потребителей информации	Анонимные форумы, чаты, доски объявлений и гостевые книги, такие как имиджборды, анонимайзеры, программы, обеспечивающие анонимизацию сетевого трафика в сети «Интернет» (tor, I2P)
5.	Отправка SMS с использованием интернет-ресурсов	Сайты, предлагающие услуги по отправке SMS-сообщений
6.	Банки рефератов, эссе, дипломных работ за исключением соответствующих задачам образования	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), представляющая собой банки готовых рефератов, эссе, дипломных работ, за исключением печатных и электронных образовательных и информационных ресурсов, создаваемых в организациях, осуществляющих образовательную деятельность
7.	Онлайн-казино и тотализаторы	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет») содержащие информацию об электронных казино, тотализаторах, игр на деньги
8.	Мошеннические сайты	Сайты, навязывающие платные услуги на базе СМС-платежей, сайты, обманным путем собирающие личную информацию (фишинг)
9.	Информация по тематике религия и атеизм, за исключением соответствующей задачам образования	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), направленные на создание и культивирование чувства превосходства носителей одной религии, религиозного или атеистического мировоззрения над любыми другими религиями или мировоззрениями
10	Магия, колдовство, чародейство, ясновидящие, приворот по фото, теургия, волшебство, некромантия, тоталитарные секты	Информационная продукция, оказывающая психологическое воздействие на детей, при которой человек обращается к тайным силам с целью влияния на события, а также реального или кажущегося воздействия на состояние

Приложение 9 к распоряжению КО
от 18.08.2014 № 108-р

_____

(Наименование ОО)

УТВЕРЖДАЮ

_____

(Должность руководителя)

_____/_____

(Подпись) (Ф.И.О.)

_____

(Дата)

Примерная форма журнала контроля за контентной фильтрацией

Дата провер-ки	**Ф.И.О. и должность проверяю-щего**	**Номер компью-тера**	**Результаты проверки**	**Принятые меры**	**Подпись проверяю-щего**

Приложение 10 к распоряжению КО
от 18.08.2014 № 108-р

Примерная форма журнала проверок антивирусной защиты

Дата провер-ки	Ф.И.О. и должность проверяю-щего	Номер компью-тера	Результаты проверки	Принятые меры	Подпись проверяю-щего

Приложение 11 к распоряжению КО
от 18.08.2014 № 108-р

Примерная инструкция по осуществлению самопроверки (мониторинга) эффективности работы системы контентной фильтрации в образовательной организации

1. Включить ПК.

2. Открыть браузер (Internet Explorer, Opera, Mozilla, Chrom).

3. Запустить Интернет-поисковик (Aport.ru, Google.ru, Rambler.ru, Mail.ru, Poisk.ru, Yandex.ru).

4. Проверить эффективность настройки СКФ на доступность сайтов порнографического характера:

4.1. Ввести в поисковой строке пользовательский запрос (например: телки, порно, мазохизм, извращение, насилие, садизм).

4.2. Просмотреть результат поиска (список ресурсов Интернет).

4.3. Ввести в поисковой строке пользовательский запрос (например: телки, порно, мазохизм, извращение, насилие, садизм).

4.4. Просмотреть результат поиска в разделе «Картинки».

4.5. Ввести в адресной строке браузера URL-адрес http://ximuk.info/index.php/2011-07-04-08-21-14 или другой, который содержит подобную информацию.

4.6. Просмотреть результат поиска.

4.7. Ввести в адресной строке IP-адрес 95.211.197.178 или другой, который содержит подобную информацию.

4.8. Просмотреть результат поиска.

4.9. Сделать вывод об эффективности работы систем контентной фильтрации в ОО.

5. Проверить эффективность настройки СКФ на доступность сайтов экстремистской направленности (повторить алгоритм работы пункта № 4 с измененными пользовательскими запросами, например: террор, хиджаб, бомба, меньшинства, рознь, бандитизм, боевики, насилие).

6. Проверить эффективность настройки СКФ на доступность сайтов, содержащих информацию об алкогольной продукции, изготовлении и использовании наркотических средств, психотропных веществ, способах совершения самоубийства (повторить алгоритм работы пункта № 4 с измененными пользовательскими запросами, например: наркотики, алкоголь, как совершить самоубийство, приобрести наркотики, галлюцинации).

7. Перейти к проверке следующего компьютера.

Примечание: осуществить проверку всех компьютеров, подключенных к сети Интернет, для исключения доступа обучающихся к сайтам, содержащим информацию, причиняющую вред здоровью и (или) развитию детей

Приложение 12 к распоряжению КО
от 18.08.2014 № 108-р

Отчет о наличии локальных правовых актов, регламентирующих доступ в сеть Интернет
(по состоянию на 05.09.2014 года)
МБОУ _____

1. Сведения о наличии локальных правовых актов и прочих документов, регламентирующих доступ в сеть Интернет

№	Критерий	Наличие докумен-та (да/нет)	Указать полные реквизиты документа
1.1	Положение о Совете образовательной организации по вопросам регламентации доступа к информации в сети Интернет		
1.2	Классификаторы информации, причиняющей вред здоровью и (или) развитию детей. (утверждаются Советом): а)классификатор информации, распространение которой запрещено в соответствии с законодательством Российской Федерации б)классификатор информации, запрещенной для распространения среди детей в)классификатор информации, распространение которой среди детей определенных возрастных категорий ограничено г)классификатор информации, не соответствующей задачам образования		
1.3	Наличие регламента организации доступа к сети Интернет		Если отдельного регламента нет, то написать, что всё прописано в правилах использования сети Интернет в ОО (п.1.10)
1.4	Наличие регламента работы с электронной почтой		
1.5	Наличие регламента организации антивирусной защиты		
1.6	Инструкция для сотрудников образовательной организации о порядке действий при осуществлении контроля использования обучающимися сети Интернет		
1.7	Инструкция пользователя по компьютерной безопасности		
1.8	Ведение журнала контроля за контентной фильтрацией		
1.9	Ведение журнала проверок антивирусной защиты		
1.10	Правила использования сети Интернет в образовательной организации		
1.11	Должностные инструкции отдельных работников образовательной организации с внесенными изменениями по использованию сети Интернет работником		

1.12	Инструкция по осуществлению мониторинга эффективности работы СКФ в образовательной организации		
1.13	Приказы по ОО о назначении ответственных за организацию работы в сети Интернет		

2. Характеристика систем контентной фильтрации в образовательной организации

№	Критерий	Значение критерия
2.1	Способ осуществления контент-фильтрации для обучающихся (осуществляется провайдером, осуществляется программными средствами, осуществляется аппаратными средствами)	
2.2	Название используемого контент-фильтра для обучающихся	
2.3	Принцип работы контент-фильтра для обучающихся (белые списки, черные списки)	
2.4	Название используемого контент-фильтра для администрации ОО	
2.5	Принцип работы контент-фильтра для администрации (белые списки, черные списки)	

Руководитель

исп.

тел.

Приложение 13 к распоряжению КО
от 18.08.2014 № 108-р

Отчет о проведении мониторинга эффективности использования систем контентной фильтрации в образовательных организациях
_____(название ОО)
за____ квартал 20___ года

1. Общие характеристики

№	Критерий	Значение критерия	Примечание
1.1	Количество компьютеров в ОО		
1.2	Количество компьютеров, имеющих выход в сеть Интернет, в т.ч.		
1.2.1	- в компьютерных классах		
1.2.2	- к которым имеется доступ обучающимся		
1.2.3	- используемых в административных целях		
1.2.4	- используемых в образовательном процессе		

2. Характеристика систем контентной фильтрации в образовательной организации

№	Критерий	Значение критерия	Примечание
2.1	Способ осуществления контент-фильтрации для обучающихся (осуществляется провайдером, осуществляется программными средствами, осуществляется аппаратными средствами)		
2.2	Название используемого контент-фильтра для обучающихся		
2.3	Принцип работы контент-фильтра для обучающихся (белые списки, черные списки)		
2.4	Название используемого контент-фильтра для администрации ОО		
2.5	Принцип работы контент-фильтра для администрации (белые списки, черные списки)		

3. Тестирование эффективности настройки программных средств, осуществляющих контентную фильтрацию в образовательных организациях

№	Критерий	Значение критерия	Примечание
3.1. Проверка эффективности настройки СКФ на доступность сайтов экстремистской направленности			
3.1.1.	Результат проверки по запросу списка ресурсов		
3.1.2.	Результат проверки по запросу картинок		
3.1.3.	Результат проверки ресурсов по URL-адресу		

3.2. Проверка эффективности настройки СКФ на доступность сайтов порнографического характера			
3.2.1.	Результат проверки по запросу списка ресурсов		
3.2.2.	Результат проверки по запросу картинок		
3.2.3.	Результат проверки ресурсов по URL-адресу		
3.3. Проверка эффективности настройки СКФ на доступность сайтов, содержащих информацию об алкогольной продукции, изготовлении и использовании наркотических средств, психотропных веществ, способах совершения самоубийства			
3.3.1.	Результат проверки по запросу списка ресурсов		
3.3.2.	Результат проверки по запросу картинок		
3.3.3.	Результат проверки ресурсов по URL-адресу		
3.4. Определение эффективности использования систем контентной фильтрации			
3.4.1.	Оценка эффективности работы СКФ в ОО (указывается в % среднее значение по п.п. 3.1.1.-3.1.3, 3.2.1.-3.2.3, 3.3.1.-3.3.3)		

4. Акт (или протокол) проверки работоспособности школьной системы контент-фильтрации (приложить)

Вывод: например, контент-фильтр работает на всех (…кол-во) компьютерах, имеющих выход в сеть Интернет. В другом случае – подробно описать состояние и что планируется.

Руководитель

исп.

тел.