Письмо Министерства просвещения Российской Федерации от 10 ноября 2025 г. N ИШ-2224/04 "О направлении методических рекомендаций"

В целях исполнения поручения Правительства Российской Федерации по вопросу разработки и направления в субъекты Российской Федерации методических рекомендаций по использованию информационно- коммуникационной сети "Интернет" в общеобразовательных организациях Минпросвещения России направляет согласованные с Минцифры России методические рекомендации по обеспечению государственных и муниципальных образовательных организаций, реализующих программы начального общего, основного общего, среднего общего и среднего профессионального образования, оптимальным и безопасным доступом к государственным, муниципальным и иным информационным системам, информационно-телекоммуникационной сети "Интернет".

Приложение: на 14 л. в 1 экз. + 1 файл в табличном формате.

И.В. Шварцман

Методические рекомендации по обеспечению государственных и муниципальных образовательных организаций, реализующих программы начального общего, основного общего, среднего общего и среднего профессионального образования, оптимальным и безопасным доступом к государственным, муниципальным и иным информационным системам, информационно-телекоммуникационной сети "Интернет"

Введение

Настоящие Методические рекомендации применяются для обеспечения в помещениях образовательных организаций, реализующих программы начального общего, основного общего, среднего общего и среднего профессионального образования (далее - ОО), оптимального и безопасного доступа к государственным, муниципальным и иным информационным системам, информационно-телекоммуникационной сети Интернет (далее - сети Интернет).

В соответствии со статьей 8 Федерального закона 29 декабря 2012 года N 273-ФЗ "Об образовании в Российской Федерации" к полномочиям органов государственной власти субъектов Российской Федерации в сфере образования относится обеспечение государственных гарантий реализации прав на получение общедоступного и бесплатного дошкольного, начального общего, основного общего, среднего общего образования в муниципальных общеобразовательных организациях и организация предоставления общего образования в государственных образовательных организациях субъектов Российской Федерации и среднего профессионального образования, включая обеспечение государственных гарантий реализации права на получение общедоступного и бесплатного среднего профессионального образования.

При разработке данных рекомендаций использованы положения следующих нормативных актов:

Федеральный закон от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

Федеральный закона от 29 декабря 2010 года N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию";

Федеральный закон от 29 декабря 2012 года N 273-ФЗ "Об образовании в Российской Федерации";

Федеральный закон от 24 июня 2025 года N 156-ФЗ "О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации";

Кодекс Российской Федерации об административных правонарушениях;

ГОСТ Р 34.12-2015 "Информационная технология. Криптографическая защита информации. Блочные шифры";

ГОСТ 34.12-2018 "Информационная технология. Криптографическая защита информации. Блочные шифры";

ГОСТ 34.13-2018 "Информационная технология. Криптографическая защита информации.

Режимы работы блочных шифров";

поручение Президента Российской Федерации от 10 июня 2023 года N Пр-1184;

поручение Президента Российской Федерации от 13 сентября 2025 года N Пр-2181;

постановление Правительства Российской Федерации от 16.04.2012 N 313 "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)";

распоряжение Правительства Российской Федерации от 12 июля 2025 года N 1880-р "Об организации, обеспечивающей создание и функционирование многофункционального сервиса обмена информацией";

приказ Минцифры России N 417, Минпросвещения России N 221 от 30 апреля 2021 г. "Об утверждении требований к подключению и доступу, включая требования к передаче данных, государственных и муниципальных образовательных организаций, реализующих программы общего и среднего профессионального образования, избирательных комиссий субъектов Российской Федерации и территориальных избирательных комиссий к единой сети передачи данных";

приказ Минпросвещения России от 02 декабря 2019 N 649 "Об утверждении Целевой модели цифровой образовательной среды";

письмо Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 12 июля 2019 года N ОИ-П19-070-15601 "О минимальных требованиях к физическим сетям для обеспечения доступом к сети Интернет образовательных организаций".

I. Перечень рекомендуемых образовательных ресурсов и сайтов для использования в образовательном процессе

Федеральные органы исполнительной власти в сфере образования (Минпросвещения России, Минобрнауки России, Рособрнадзор) формируют перечень рекомендуемых ресурсов и направляет в субъекты Российской Федерации для включения в разрешенный перечень ресурсов (далее - белый список) для использования в образовательном процессе, во внеурочное время или для использования образовательными организациями (в том числе сервисы федеральной государственной информационной системы "Моя школа", электронные образовательные ресурсы, федеральные сайты и порталы образовательной и воспитательной направленности). Белый список федеральных ресурсов является доступным для пользователей на всей территории Российской Федерации.

В соответствии с требованиями Федерального закона от 24.06.2025 N 156-ФЗ "О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации" и распоряжения Правительства Российской Федерации от 12.07.2025 N 1880-р должно быть обеспечено осуществление с использованием "Цифровой платформы MAX" организации взаимодействия участников образовательных отношений при реализации основных общеобразовательных программ, образовательных программ среднего профессионального образования и дополнительных общеобразовательных программ, в том числе с использованием региональных информационных систем в сфере общего образования, среднего профессионального образования и дополнительного образования детей и взрослых, федеральных информационных систем в системе образования, единой системы идентификации и аутентификации и федеральной государственной информационной системы "Единый портал государственных и муниципальных услуг (функций)".

Заинтересованные федеральные органы исполнительной власти направляют в один из ответственных федеральных органов исполнительной власти в сфере образования по сфере ведения предложения для внесения ресурсов в белый список.

Субъекты Российской Федерации самостоятельно определяют перечень региональных ресурсов белого списка с учетом предложений образовательных организаций, функционирующих на их территории, и направляют данный перечень в адрес поставщика услуг связи доступа к сети Интернет для образовательных организаций на территории субъекта Российской Федерации.

Справочно: актуальный белый список ресурсов прилагается.

II. Правила фильтрации контента для обеспечения защиты от нежелательной информации

При осуществлении в образовательных организациях доступа к информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") оператором связи должно обеспечиваться ограничение доступа к сайтам в сети "Интернет", содержащим информацию, распространение которой в Российской Федерации запрещено, в соответствии с требованиями ст. 15.1-15.9 Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

Помимо этого, в соответствии с требованиями Федерального закона от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" (далее - Федеральный закон N 436-ФЗ) при осуществлении в образовательных организациях доступа детей к сети "Интернет" должно быть обеспечено ограничение доступа к информации, причиняющей вред здоровью и (или) развитию детей (далее - нежелательная информация). Виды нежелательной информации определены частями 2 и 3 статьи 5 Федерального закона N 436-ФЗ:

а) информация, запрещенная для распространения среди детей:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий;

- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, никотинсодержащую продукцию, сжиженные углеводородные газы, содержащиеся в потенциально опасных газосодержащих товарах бытового назначения, и (или) их пары, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

- 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 N 436-ФЗ;

- содержащая изображение или описание сексуального насилия;

- оскорбляющая человеческое достоинство и общественную нравственность, выражающая явное неуважение к обществу, содержащая изображение действий с признаками противоправных, в том числе насильственных, и распространяемая из хулиганских, корыстных или иных низменных побуждений;

- отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

- пропагандирующая либо демонстрирующая нетрадиционные сексуальные отношения и (или) предпочтения;

- пропагандирующая педофилию;

- способная вызвать у детей желание сменить пол;

- пропагандирующая отказ от деторождения;

- оправдывающая противоправное поведение;

- содержащая нецензурную брань;

- содержащая информацию порнографического характера;

- 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, позволяющую прямо или косвенно установить личность такого несовершеннолетнего;

- содержащаяся в информационной продукции, произведенной иностранным агентом;

б) информация, распространение которой среди детей определенных возрастных категорий ограничено:

- представляемая в виде изображения или описания жестокости, физического и (или) психического насилия (за исключением сексуального насилия), преступления или иного антиобщественного действия;

- 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;

- представляемая в виде изображения или описания половых отношений между мужчиной и

женщиной;

- содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Для обеспечения защиты от нежелательной информации рекомендуется при использовании детьми сети "Интернет" производить в режиме реального времени проверку ресурсов сети "Интернет", доступ к которым осуществляется детьми, и блокировку нежелательной информации (далее - контентная фильтрация) путем применения:

- "белых списков" (перечней ресурсов сети "Интернет", доступ к которым разрешен);

- "черных списков" (перечней ресурсов сети "Интернет", доступ к которым заблокирован);

- семантического и морфологического анализа содержимого ресурсов сети "Интернет" для определения необходимости их блокировки при наличии на таком ресурсе признаков, позволяющих отнести его содержимое к нежелательной информации.

В целях обеспечения защиты детей от нежелательной информации при осуществлении доступа к сети "Интернет" рекомендуется использование системы (сервиса) контентной фильтрации, позволяющей производить в режиме реального времени проверку ресурсов сети "Интернет", доступ к которым осуществляется детьми, и блокировку нежелательной информации.

Для системы (сервиса) контентной фильтрации рекомендуется наличие следующих функций и возможностей:

- контентная фильтрация входящего и исходящего трафика сети "Интернет" по протоколам HTTP/HTTPS;

- блокировка злонамеренных ресурсов сети "Интернет";

- поддержка "черных списков" и "белых списков" ресурсов сети "Интернет";

- блокировка вредоносного программного обеспечения и нежелательной рекламы;

- обеспечение антивирусной защиты пользователей при взаимодействии с ресурсами сети "Интернет" (веб-антивирус), включая анализ содержимого веб-ресурсов и получаемых/передаваемых вложений;

- принудительное включение безопасного поиска для поисковых систем в целях блокировки нежелательной информации;

- осуществление журналирования поисковых запросов пользователей на срок до 6 месяцев;

- блокировка приложений популярных социальных сетей с возможностью открытия к ним доступа по запросам образовательных организаций для страниц каждой отдельно взятой социальной сети, при условии поддержки социальной сетью разграничения действий внутри сервиса;

- возможность добавления ресурсов сети "Интернет" в "белый список" и "черный список" по запросам уполномоченных органов государственной власти, образовательных организаций;

- возможность использования аутентификации пользователей сети "Интернет" посредством федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" для определения параметров осуществления контентной фильтрации.

Справочно:

частью 2 статьи 6.17 Кодекса Российской Федерации об административных правонарушениях предусмотрена ответственность за неприменение лицом, организующим доступ к распространяемой посредством информационно-телекоммуникационных сетей (в том числе сети "Интернет") информации (за исключением операторов связи, оказывающих эти услуги связи на основании договоров об оказании услуг связи, заключенных в письменной форме) в местах, доступных для детей, административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию, в виде административного штрафа на юридических лиц от 20 000 до 50 000 рублей.

III. Меры по контролю доступа к сети "Интернет" в образовательных организациях

В целях обеспечения защиты от нежелательной информации доступ к сети "Интернет" для пользователей образовательной организации осуществляется с обязательным применением контентной фильтрации. Отключение контентной фильтрации может производиться для пользователей из числа педагогического состава и административно-хозяйственного персонала образовательных организаций, а также иных совершеннолетних пользователей путем аутентификации пользователя на базе учетных записей портала "Госуслуги" (ЕСИА), а также для конкретных IP-адресов по заявке образовательной организации.

IV. Обеспечение доступа и защиты к сети Интернет

Уполномоченный орган исполнительной власти субъекта Российской Федерации обеспечивает оптимальный доступ для образовательных организаций к сети Интернет, но не ниже установленной поручением Президента Российской Федерации от 10 июня 2023 г. N Пр-1184 по вопросу обеспечения образовательных организаций, находящихся в труднодоступных населенных пунктах, подключением к информационным системам и к сети Интернет с использованием единой сети передачи данных со скоростью подключения не ниже скоростей подключения, действовавшим в этих организациях в рамках федеральных контрактов:

1. Параметры подключения образовательных организаций к сетям связи:

1.1. для объектов образовательных организаций, расположенных в городских поселениях и подключенных с использованием волоконно-оптических линий связи (далее - ВОЛС), обеспечена пропускная способность канала связи не менее 100 Мбит/с;

1.2. для объектов образовательных организаций, расположенных в сельских поселениях и подключенных с использованием ВОЛС, обеспечена пропускная способность канала связи не менее 50 Мбит/с;

1.3. для объектов образовательных организаций, подключенных без использования ВОЛС посредством иных линий связи (в том числе спутниковых), обеспечена пропускная способность канала связи не менее 1 Мбит/с.

1.4. При передаче трафика образовательных организаций поддерживаются 3 класса обслуживания:

- Класс 1 - трафик приложений реального времени (голос, видео), критичный к потерям пакетов, задержкам и колебаниям задержки;
- Класс 2 - трафик информационных систем, критичный к задержкам и потерям;
- Класс 3 - трафик, некритичный к задержкам ("Интернет", различные сетевые службы).

При превышении трафиком Класса 1 пропускной способности, установленной на порту для Класса 1, должен производиться сброс пакетов с качеством Класса 3; при превышении трафиком Класса 2 пропускной способности, установленной на порту для Класса 2, - сброс пакетов с качеством Класса 3; при превышении трафиком Класса 3 пропускной способности порта - сброс пакетов

Рекомендуемые параметры качества передачи L2-пакетов через канал связи, организованный посредством ВОЛС:

Тип трафика	Процент потерянных L2-пакетов, не более	Задержка передачи L2-пакетов в одну сторону, не более	Вариация задержки, не более
Класс 1	0,2%	15 мс	10 мс
Класс 2	0,2%	20 мс	не нормируется
Класс 3	5%	25 мс	не нормируется

Задержка передачи L2-пакета через канал связи в каждом направлении при наличии в канале спутниковой составляющей не превышает 400 мс.

2. Защита информации:

2.1. при осуществлении передачи данных для доступа образовательных организаций к государственным, муниципальным и иным информационным системам, в которых осуществляется обработка персональных данных, обеспечивается криптографическая защита информации с учетом требований следующих документов:

- Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), утвержденное постановлением Правительства Российской

Федерации от 16.04.2012 N 313;

- ГОСТ Р 34.12-2015 "Информационная технология. Криптографическая защита информации. Блочные шифры";

- ГОСТ 34.12-2018 "Информационная технология. Криптографическая защита информации. Блочные шифры";

- ГОСТ 34.13-2018 "Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров".

3. Информационная безопасность:

3.1. при осуществлении передачи данных для доступа образовательных организаций к сети "Интернет" обеспечивается защита от DDoS-атак[1] следующих типов:

- атаки на переполнение каналов связи (Volumetric Attacks);

- атаки на сетевую инфраструктуру (State Exhaustion Attacks);

- атаки уровня приложений (Application Attacks);

3.2. при осуществлении передачи данных для доступа образовательных организаций к сети "Интернет" применяется межсетевое экранирование, обеспечивающее информационную безопасность внутренних сегментов локальных вычислительных сетей образовательных организаций при осуществлении межсетевого взаимодействия с внешними сетями передачи данных, в том числе сетью "Интернет", для предотвращения несанкционированного доступа к внутренним сегментам локальных вычислительных сетей образовательных организаций и вредоносного воздействия на них.

4. Мониторинг параметров качества оказываемых услуг связи:

4.1. для услуг связи, оказываемых образовательным организациям, осуществляется мониторинг параметров качества, включающий в себя:

- объективный контроль работоспособности средств связи на объектах образовательных организаций с использованием сертифицированных и поверенных средств измерения;

- отображение в режиме реального времени информации о статусе и параметрах услуг связи на объектах образовательных организаций;

- формирование отчетности о статусе и параметрах услуг связи, утилизации (потреблению) трафика, качестве фактически оказанных услуг связи для объектов образовательных организаций.

5. Рекомендации к технической поддержке:

5.1. Осуществляется техническая поддержка образовательных организаций по вопросам оказания услуг связи в соответствии с регламентом технической поддержки.

5.2. Регламент технической поддержки предусматривает порядок взаимодействия между образовательной организацией, оператором связи и заказчиком по государственному контракту, в том числе:

- порядок регистрации, открытия, обработки и закрытия обращений образовательных организаций по вопросам оказания услуг связи;

- порядок взаимодействия образовательных организаций, оператора связи и заказчика по государственному контракту при планировании и проведении технологических перерывов;

- порядок формирования и предоставления отчетности по обращениям образовательных организаций и отчетности о качестве услуг связи.

5.3. В целях оказания дополнительной консультационной поддержки образовательных организаций по вопросам, связанным с оказанием услуг связи, а также в целях обеспечения возможности управления услугами связи со стороны образовательных организаций, используется общедоступный ресурс в сети "Интернет", на котором размещаются инструкции и дополнительные материалы для образовательных организаций по вопросам оказания услуг связи, а также личный кабинет для представителей образовательных организаций.

5.4. Техническая поддержка осуществляется круглосуточно и ежедневно.

5.5. Обращения в техническую поддержку регистрируются посредством следующих способов:

- по бесплатному контактному номеру телефона;

- посредством отправки сообщений электронной почты на единый почтовый ящик;

- посредством личного кабинета;

5.6. автоматическое заведение инцидентов на основании событий, полученных в ходе мониторинга параметров качества оказываемых услуг связи (пункт 4 раздела IV настоящих Методических рекомендаций).

5.7. При проведении профилактических работ на оборудовании и сетях связи допускается перерыв в оказании услуг связи. Проведение профилактических работ осуществляется в часы наименьшей нагрузки. При этом производится информирование представителя образовательной организации и заказчика по государственному контракту не менее чем за 3 рабочих дня до начала профилактических работ по телефону или электронной почте.

5.8. Приоритеты и время восстановления работоспособности услуг связи:

5.8.1. Неисправности подразделяются на яетырч приоритета по степени срочности их устранения:

1-ый приоритет - Критичный:

- услуга не доступна (авария);

- массовые (более десяти обращений в течение тридцати минут от различных образовательных организаций в одном субъекте Российской Федерации) обращения в техническую поддержку, связанные с нарушением работоспособности услуг связи, относящиеся к одному событию;

- время устранения неисправности - 10 часов рабочего времени с момента регистрации обращения;

- часы устранения неисправности - с 08:00 до 18:00 местного времени по рабочим дням (ежедневно за исключением выходных и нерабочих праздничных дней), круглосуточно - в дни проведения единого государственного экзамена.

2-ой приоритет - Высокий:

- наблюдается массовая деградация производительности или периодическое прерывание услуги не менее чем в 5 процентах общего числа образовательных организаций в одном субъекте Российской Федерации;

- фиксируются периодические прерывания или деградация (снижение скорости относительно заявленной) в работе услуги в одной образовательной организации;

- время устранения неисправности - 14 часов рабочего времени с момента регистрации обращения;

- часы устранения неисправности - с 08:00 до 18:00 местного времени по рабочим дням (ежедневно за исключением выходных и нерабочих праздничных дней), круглосуточно - в дни проведения единого государственного экзамена.

3-й приоритет - Средний:

- нарушение вспомогательной функциональности услуг связи;

- запрос на обслуживание или изменение настроек;

- запрос на изменение конфигурации или функциональности услуг связи;

- время устранения неисправности - 20 часов рабочего времени с момента регистрации обращения;

- часы устранения неисправности - с 08:00 до 18:00 местного времени по рабочим дням (ежедневно за исключением выходных и нерабочих праздничных дней).

4-й приоритет - Низкий:

- проблемы без утраты способности услуг связи;

- запросы по оказанию информационной поддержки;

- представителю образовательной организации требуется консультация;

- время устранения неисправности - 24 часа рабочего времени с момента регистрации обращения;

- часы устранения неисправности - с 08:00 до 18:00 местного времени по рабочим дням (ежедневно за исключением выходных и нерабочих праздничных дней).

Время устранения неисправности указано для случаев, не требующих выезда. Для восстановления магистральной кабельной инфраструктуры, работ на узловом и магистральном оборудовании, замены оборудования / восстановления кабельной инфраструктуры и иных работ, требующих выезда, нормативные сроки решения инцидента увеличиваются на 48 часов. Указано время для восстановительных работ инфраструктуры оператора связи, без учета времени восстановительных работ оборудования образовательной организации, инфраструктуры информационных систем, а также нахождения образовательной организации в труднодоступном населенном пункте.

Для объектов, расположенных в труднодоступных населенных пунктах (труднодоступный населенный пункт - это населенный пункт, который в силу погодных, природных, техногенных и иных обстоятельств и (или) отсутствия элементов инфраструктуры становится недоступным или труднодостижимым для транспортных средств), срок решения инцидента для восстановления кабельной инфраструктуры, замены оборудования и иных работ, требующих выезда, а также для восстановления магистральной кабельной инфраструктуры, работ на узловом и магистральном оборудовании, увеличивается на 9 рабочих дней.

В случаях, если для решения заявки требуется дополнительная информация от образовательной организации или проверка работоспособности с ее стороны, время простоя не учитывается до получения запрошенной информации.

5.9. Порядок увеличения пропускной способности каналов связи:

Информация о загрузке канала доступа в сеть "Интернет" предоставляется оператором связи на

основе мониторинга канала связи. Если в течение одного месяца более двух раз и не менее, чем на 30 последовательных минут, достигалось предельное значения загрузки канала на уровне пропускной способности для данной образовательной организации, то для данной образовательной организации рекомендуется произвести увеличение пропускной способности канала связи при наличии технической возможности.

V. Обучение педагогов и учащихся основам цифровой грамотности и безопасности в сети

Субъектам Российской Федерации в рамках проводимых мероприятий по повышению квалификации педагогических кадров рекомендуется включить в программы повышения квалификации педагогических кадров модуль по основам цифровой грамотности и безопасности в сети Интернет.

Для обучающихся образовательных организаций рекомендуется проводить на регулярной основе обучающие мероприятия по основам цифровой грамотности и безопасности в сети Интернет.

Субъекты Российской Федерации обеспечивают участие педагогических работников и обучающихся образовательных организаций во всероссийских мероприятиях цифровой направленности (олимпиада по искусственному интеллекту, "Урок цифры", "Битва роботов" и т.д.), способствующих повышению культуры корректного пользования цифровыми ресурсами.

---

[1] DDoS-атака - Distributed Denial of Service, распределенная атака на отказ в обслуживании, разновидность атак на компьютерные системы и сети связи, связанных с большим количеством запросов (в виде IP-пакетов), посылаемых с большого количества IP-адресов сети "Интернет" и направленных на IP-адреса объектов атаки.