

О принятии мер, направленных на обеспечение защиты детей от информации, причиняющей вред их здоровью и развитию

В последнее десятилетие вопросы обеспечения благополучного и защищенного детства стали одними из основных национальных приоритетов Российской Федерации.

В результате значительного повышения обеспеченности россиян компьютерами и подключения в рамках национального проекта школ к сети «Интернет» пользовательская активность российских школьников резко возросла.

Бесспорно Интернет – это наш сегодняшний день и при правильном использовании – это возможность получать новые полезные знания. Однако всего 44% несовершеннолетних используют Интернет как источник информации для учебы.

В силу отсутствия жизненного опыта, неокрепшей психики, ребенок более других подвержен воздействию через компьютерные игры, мобильную связь, рекламу, и особенно, через всемирную паутину сети «Интернет».

В Федеральном законе от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию, введено понятие информационной безопасности детей, рассмотрены виды информации, причиняющей вред здоровью и (или) развитию детей».

Комплекс мер, направленных на обеспечение информационной безопасности детства, закреплен в «Национальной стратегии действий в интересах детей на 2012-2017 годы», утвержденной указом Президента РФ от 01.06.2012 №761 (далее — Национальная стратегия действий в интересах детей)

состоялось заседание коллегии прокуратуры области, на котором рассмотрен вопрос о результатах проверки исполнения законодательства, обеспечивающего защиту детей от информации, наносящей вред их здоровью, нравственному и духовному развитию, что говорит об актуальности данного вопроса.

С позиций системы образования информационная безопасность обучающихся – это необходимость:

1. обеспечивать достаточные и защищенные информационные ресурсы и информационные потоки для поддержания образовательного процесса на соответствующем уровне;
2. противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику обучающихся;
3. вырабатывать личностные и групповые навыки и умения безопасного поведения;
4. поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно не было навязано.

Таким образом, информационная безопасность детей включает две относительно самостоятельные составляющие – гуманитарную и техническую.

Техническая составляющая включает организационно-правовые механизмы и технические средства защиты.

Гуманитарная составляющая включает содержание и организацию образовательного процесса, подготовку педагогов, работу с родителями.

Проблема защиты детей от информации, причиняющей вред их здоровью и развитию, в Российской Федерации регулируется следующими нормативно правовыми актами:

- Конституция РФ от 12.12.1993;
- Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе»;
- Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»;
- Указ Президента РФ от 01.06.2012 г. № 761 «О Национальной стратегии действий в интересах детей на 2012-2017 годы»;
- Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Минобрнауки РФ от 11.05.2011 №АФ-12/07 вн.

На региональном уровне деятельность образовательных организаций по информационной защите детей регулируется следующими нормативно правовыми актами:

-

На уровне **Образовательной организации**

1. Вопросы использования возможностей сети «Интернет» в образовательном процессе рассмотреть на педсовете;
2. Издать приказы по вопросам обеспечения информационной безопасности обучающихся;
3. Разработать локальные акты (*Регламент доступа в сеть «Интернет», Правила использования сети «Интернет», Положение о Совете образовательной организации по вопросам регламентации доступа к информации в сети «Интернет» и др.*);
4. Разработать или внести необходимые дополнения в должностные инструкции (*сотрудника, назначенного ответственным за организацию работы с сетью «Интернет» и контроль доступа в сеть; учителя, допущенного к работе в сети*);
5. Разработать и внедрить программы обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет-зависимости, предупреждения рисков вовлечения в противоправную деятельность.

Внешняя защищенность образовательной среды реализуется через:

- Создание системы контентной фильтрации, которая представляет собой программный комплекс, позволяющий ограничить учащимся доступ к интернет-ресурсам;
- Использование различных систем противовирусной защиты;
- Использование специальных настроек операционной системы;
- Установку поисковых систем для детей.

Компанией ОАО «Ростелеком» в рамках договора об оказании услуг по передаче данных организована централизованная контентная фильтрация ресурсов сети «Интернет».

В качестве дополнительных средств контентной фильтрации департамент рекомендует программные продукты: *Интернет цензор* (<http://icensor.ru>), *НетПолис* (<http://www.netpolice.ru>) (для операционной системы Windows), *Дансгардиан* (<http://dansguardian.org>) (для операционной системы Linux).

В Национальной стратегии действий в интересах детей закреплён ряд мер, направленных на обеспечение информационной безопасности детства.

Одной из таких мер, заявлено внедрение системы мониторинговых исследований по вопросам обеспечения безопасности образовательной среды образовательной организации.

Вышеуказанные мониторинговые исследования в основном предполагают:

- 1) Мониторинг функционирования и использования программного продукта, обеспечивающего контент-фильтрацию Интернет-трафика;
- 2) Проведение сверки имеющегося библиотечного фонда и поступающей литературы с федеральным списком экстремистских материалов.

Департамент образования и науки рекомендует 1 раз в четверть проводить контроль работы средств контентной фильтрации и сверку библиотечного фонда силами общественности и активировать, полученные результаты. Если в ходе проверки удалось выйти на запрещенную информацию, адрес ресурса активируется и направляется провайдеру, предоставляющему услугу доступа в сеть. Особое внимание следует уделить доступу к информации, содержащейся в федеральном списке экстремистских материалов.

Формирование у подростка готовности и способности регулировать информационные опасности вокруг себя одна из задач системы образования.

Для решения этой задачи образовательная организация разрабатывает программы обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет-зависимости, предупреждения рисков вовлечения в противоправную деятельность.

Оценивая собственную подготовку по вопросам обеспечения информационной безопасности детей 89% педагогов отмечают, что знают о существовании основных законодательных актов, но не знакомы с их основными положениями; почти все участники опроса (98%) уверены, что педагогу необходима специальная подготовка к работе с детьми и родителями по вопросам информационной безопасности. В связи с чем, проблема повышения квалификации педагогов приобретает особую актуальность.

Еще одной мерой, направленной на обеспечение информационной безопасности детства, является создание порталов и сайтов, аккумулирующих сведения о лучших ресурсах для детей и родителей; стимулирование родителей к использованию услуги «Родительский контроль», позволяющей устанавливать ограничения доступа к сети «Интернет».

Родительский контроль – это услуга фильтрации контента, размещенного в сети «Интернет» для обеспечения доступа детей только к безопасной, проверенной информации. Информацию об услуге и способах её подключения можно получить на официальном сайте провайдера и у учителей информатики ОО.

В целях усиления профилактической работы по вопросу защиты детей от информации, причиняющей вред их здоровью в образовательной организации проводятся следующие мероприятия:

1. родительские собрания на тему «Защита детей от информации, наносящей вред их здоровью, нравственному и духовному развитию». Особое внимание уделяется разъяснению необходимости подключения домашней услуги «Родительский контроль».
2. Оформляется стенд для родителей, разместив на нем материалы по защите детей от информации, приносящей вред их здоровью и развитию, в том числе, информацию об услуге «Родительский контроль».
3. Размещаются информации для родителей (законных представителей) и обучающихся на официальном сайте образовательной организации.

Помимо услуги «Родительский контроль» родителям предлагается **NetKids** — сервис, который позволяет контролировать использование сети «Интернет» детьми.

Чтобы обезопасить детей от информации, разрушающей детскую психику, созданы специальные детские поисковые системы, которые индексируют не все сайты, а только сайты с детской или околодетской тематикой. Например, детский браузер Гоголь, поисковая система «АгА», интерактивное облако подсказок, детский портал KINDER online.ru.

На заре появления социальных сетей основной их аудиторией была молодежь, сейчас же в социальных сетях общаются люди самого разного возраста. Стоит ли говорить, что контент социальных сетей далеко не всегда приемлем для детей, добравшихся до интернета. Эксперты признали «ВКонтакте» самой опасной социальной сетью. Однако есть специальные **детские социальные сети**, содержание которых соответствует возрасту юных пользователей.

Ответственность образовательной организации по вопросу обеспечения информационной безопасности детей закреплена в Федеральных законах от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации» и от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

В соответствии с п.15 ч.3 ст.28 Федерального закона «Об образовании в Российской Федерации» к компетенции образовательной организации 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 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.

В соответствии с Приказом Генеральной прокуратуры РФ «Об организации прокурорского надзора за исполнением законов о несовершеннолетних и молодежи» от 26 ноября 2007 г. №188, соблюдение законодательства о защите детей от информации, наносящей вред их здоровью, репутации, нравственному и духовному развитию в деятельности средств массовой информации, органов и учреждений образования и культуры проверяется систематически.

В период с 20 августа по 31 декабря 2015 г. сотрудниками службы по контролю и надзору в области образования было проведено **57** проверок в части исполнения законодательства, обеспечивающего защиту детей от информации, наносящей вред их здоровью, нравственному и духовному развитию.

В рамках проверок образовательных организаций изучались следующие вопросы:

- Организация доступа в сеть «Интернет»;
- Административные и организационные меры, технические и программно-аппаратные средства защиты детей от вредной информации;
- Внедрение программ обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет-зависимости, предупреждения рисков вовлечения в противоправную деятельность;
- Внедрение системы мониторинговых исследований по вопросам обеспечения безопасности образовательной среды образовательной организации;
- Защита детей от запрещённой для распространения информации в рекламе.

В ходе проверок выявлены следующие нарушения:

- В ряде образовательных организаций отсутствуют средства контент-фильтрации (СКФ) на компьютерах, имеющих выход в сеть «Интернет» (*в том числе на компьютерах, детей-инвалидов, обучающихся дистанционно*) или установленные СКФ не в полной мере обеспечивают фильтрацию;
- Отсутствуют локальные акты, регламентирующие организацию работы по защите детей от противоправного контента в образовательной среде;
- В локальных актах неправомерно закреплено, что школа не несет ответственность за случайный доступ к информации не совместимой с задачами обучения и воспитания, размещенной не на Интернет-ресурсах школы.
- В локальных актах закреплена материальная ответственность пользователя при нанесении ущерба и наказание пользователя лишением возможности выхода в сеть «Интернет» за административное нарушение.

Однако Гражданский кодекс (статьи 1073, 1074) предусматривает различные правила гражданско-правовой ответственности за вред, причинённый несовершеннолетними в возрасте до 14 лет и несовершеннолетними в возрасте от 14 до 18 лет.

- В библиотеках образовательных организаций отсутствует федеральный список экстремистских материалов с последними изменениями;
- Сверки имеющегося библиотечного фонда и поступающей литературы с федеральным списком экстремистских материалов не проводятся, Службой по

результатам проверок в образовательные организации направлены предписания с требованиями устранения выявленных нарушений и причин, способствующих их совершению, в ряде случаев с предложением о привлечении к дисциплинарной ответственности виновных должностных лиц.

Сегодняшнее региональное информационное пространство формируется на различных уровнях и все они важны для обеспечения информационной безопасности обучающихся. Безопасность жизнедеятельности учащегося может быть обеспечена только на основе сознательно проектируемого и прогнозируемого процесса управления информационными воздействиями в образовательном пространстве региона.

Заместитель директора департамента А.П. Балахонов