Организация безопасной информационной образовательной среды в образовательной организации

Учебно-методическое пособие

Государственное бюджетное образовательное учреждение
дополнительного профессионального образования
«НИЖЕГОРОДСКИЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ»

Организация безопасной информационной образовательной среды *в* образовательной организации

Учебно-методическое пособие

Нижний Новгород
Нижегородский институт развития образования
2018

УДК 371
ББК 4313.5я431
О-64

Авторы-составители:
Е. Г. Калинкина, канд. пед. наук, доцент, первый проректор ГБОУ ДПО НИРО;
Ю. Ю. Абышева, канд. социол. наук, директор направления департамента внешних коммуникаций ПАО «Ростелеком»;
Т. И. Канянина, канд. пед. наук, доцент, зав. кафедрой информационных технологий ГБОУ ДПО НИРО;
С. Ю. Степанова, ст. преподаватель кафедры информационных технологий ГБОУ ДПО НИРО;
И. Н. Лескина, канд. пед. наук, руководитель Центра социально-педагогических измерений в образовании ГБОУ ДПО НИРО;
В. Б. Клепиков, канд. пед. наук, ст. преподаватель кафедры информационных технологий ГБОУ ДПО НИРО

Рецензент
М. Ю. Втюрин, канд. физ.-мат. наук, зав. кафедрой теории и методики обучения информатике ГБОУ ДПО НИРО

ISBN 978-5-7565-0759-1

Введение

XXI век ознаменован фундаментальным развитием информационных и коммуникационных технологий, глобальной сети Интернет и информационного общества. Использование информационных технологий во всех сферах жизни и деятельности человека требует от системы образования идти по пути внедрения информационных технологий в образовательный процесс, что актуализирует создание безопасной информационной образовательной среды (БИОС) образовательных организаций.

Содержание понятия «информационная среда» понимается рядом авторов как специально созданная и определенным образом структурированная часть информационного пространства, включающего совокупность субъектов, создающих, перерабатывающих, использующих информацию, саму информацию и аппаратные средства, ее обслуживающие. Таким образом, информационная образовательная среда (ИОС) — это информационная среда, целенаправленно создающаяся для осуществления образовательного процесса.

Одной из особенностей информационного общества является противоречие между колоссальными возможностями воздействия на социальную организацию и сознание человека, предоставляемыми новыми информационными технологиями, с одной стороны, и угрозами их использования в деструктивных по отношению к индивидууму или социальной группе целях, с другой. Комплекс вызовов и угроз современного мира не обходит стороной и ИОС.

Анализ возможных информационных угроз позволяет сделать вывод о том, что многие из них непосредственно влияют на построение, структуру, содержание, функционирование информационной образовательной среды. В этой связи актуальной задачей представляется поиск действенных технологий обеспечения защищенности электронных образовательных ресурсов, образовательного контента и информационной образовательной среды в целом.

Объем и влияние информации, доступной учащемуся, возросли настолько, что правомерным становится говорить об информационной социализации личности, а сама информация, таким образом, превращается в один из ведущих факторов социализации, такой же мощный, как семья или школа. В этих условиях наиболее незащищенными являются дети и подростки, молодежь, еще не выработавшая строгого мировоззрения, четкой жизненной позиции.

На личность ребенка в современном информационном обществе воздействует мощный информационный поток. Во-первых, это информация, которую предлагают учителя, родители, психологи, педагоги дополнительного образования. Данная информация тщательно обрабатывается и фильтруется, прежде чем передаваться обучающемуся. Во-вторых, учащийся получает информацию из внешней информационной среды, которая включает в себя Интернет, средства массовой информации (СМИ), различные коммуникации в виртуальном сообществе и пр. Данная информация дается ученику в «сыром» виде, и от его личностных характеристик и особенностей зависит, в каком виде она будет переработана, принята или отсеяна, насколько он сможет противостоять угрозам и опасностям инфокоммуникационной окружающей среды.

Рост числа угроз и опасностей в образовательной среде, вызовов обществу и системе образования требует кардинальных действий по обеспечению безопасности ИОС и БИОС.

БИОС представляет собой совокупность технических, программных, телекоммуникационных и методических средств, систему психолого-педагогических, материальных и организационных условий, позволяющих применять в образовательном процессе информационные технологии, обеспечивающие защищенность личности от негативного воздействия информационных факторов и оптимальность взаимодействия ее с информационной образовательной средой.

Обязательными условиями функционирования безопасной информационной образовательной среды являются за-

щищенность ресурсов и пользователей БИОС от негативного и деструктивного воздействия со стороны внешних и внутренних опасных факторов, сохранение постоянного и непрерывного доступа пользователей ко всем педагогическим технологиям и ресурсам БИОС, сохранение функциональности БИОС в условиях повседневного цикла жизнедеятельности.

Таким образом, безопасная информационная образовательная среда представляет собой систему, которая включает материально-технические, информационные и кадровые ресурсы; обеспечивает автоматизацию управленческих и педагогических процессов, согласованную обработку и использование информации, полноценный безопасный информационный обмен; предполагает наличие нормативно-организационной базы, технического и методического сопровождения функционирования БИОС.

Эффективное обеспечение безопасности ИОС возможно только в рамках реализации системного подхода, предполагающего сочетание мер следующих уровней:

- нормативно-правового;
- административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- организационно-управленческого (меры безопасности, ориентированные на людей);
- программно-технического;
- организационно-методического. ☺

КОНЦЕПТУАЛЬНЫЕ И СОДЕРЖАТЕЛЬНЫЕ ОСОБЕННОСТИ СОЗДАНИЯ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Нормативно-правовое обеспечение создания безопасной информационной образовательной среды образовательной организации

Создание безопасной информационной образовательной среды образовательной организации является важнейшим условием реализации Федерального государственного образовательного стандарта (ФГОС) соответствующей ступени обучения. В этой связи рассмотрим определение ИОС, приведенное в стандарте (как ее правовое толкование и выражение): «Информационно-образовательная среда образовательного учреждения включает: комплекс информационных образовательных ресурсов, в том числе цифровые образовательные ресурсы, совокупность технологических средств информационных и коммуникационных технологий (ИКТ): компьютеры, иное ИКТ-оборудование, коммуникационные каналы, систему современных педагогических технологий, обеспечивающих обучение в современной информационно-образовательной среде».

Вопросы обеспечения безопасной информационной образовательной среды современной образовательной организации находят отражение в следующих нормативных документах федерального и регионального уровней.

Федеральный уровень

➠ Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ. В соответствии с законом в организациях, осуществляющих образовательную деятельность:

— при реализации образовательных программ с применением исключительно электронного обучения, дистанционных образовательных технологий в организации, осуществляющей образовательную деятельность, должны быть созданы условия для функционирования электронной информационно-образовательной среды, включающей в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств и обеспечивающей освоение обучающимися образовательных программ в полном объеме независимо от места нахождения обучающихся;

— при реализации образовательных программ с применением электронного обучения, дистанционных образовательных технологий организация, осуществляющая образовательную деятельность, обеспечивает защиту сведений, составляющих государственную или иную охраняемую законом тайну.

В этом контексте особую важность представляет именно фактор безопасности ИОС, обеспечивающий защиту субъектов образовательного процесса от «методов и средств обучения и воспитания, образовательных технологий, наносящих вред физическому или психическому здоровью обучающихся».

➠ Федеральный закон № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации». Регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; при применении информационных технологий, а также при обеспечении защиты информации.

➠ Федеральный закон № 531-ФЗ от 31.12.2014 «О вне-

сении изменений в статьи 13 и 14 Федерального закона "Об информации, информационных технологиях и о защите информации"». Вносит изменения и дополнения в ряд статей 149-ФЗ от 27.07.2006.

➠ Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 года № 436-ФЗ. Регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции.

➠ Федеральный закон от 27.06.2006 г. № 152-ФЗ «О персональных данных». В соответствии с законом в России существенно возрастают требования ко всем частным и государственным компаниям и организациям, а также физическим лицам, которые хранят, собирают, передают или обрабатывают персональные данные (в том числе фамилию, имя, отчество). Такие компании, организации и физические лица относятся к операторам персональных данных. Согласно закону операторы персональных данных должны выполнить ряд требований по защите персональных данных физических лиц, обрабатываемых в информационных системах организации.

➠ Федеральный государственный образовательный стандарт основного общего образования (утвержден приказом Минобрнауки России от 17 декабря 2010 г. № 1897).

➠ Федеральный государственный образовательный стандарт основного общего образования (ФГОС ООО). В свете ФГОС ООО «информационно-методические условия реализации основной образовательной программы основного общего образования должны обеспечиваться современной информационно-образовательной средой». В этой связи создание ИОС образовательной организации, открытой для внедрения инновационных образовательных продуктов и технологий и вместе с тем безопасной для субъектов образовательного процесса, является одним из приоритетных направлений системы образования в условиях информационного общества.

➠ Профессиональный стандарт «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)» (утвержден приказом Министерства труда и социальной защиты РФ № 544н от 18 октября 2013 года, дополнен приказом № 422н от 05.08.2016 г.). Профессиональный стандарт педагога выделяет его умение «проектировать психологически безопасную и комфортную образовательную среду».

➠ Государственная программа Российской Федерации «Развитие образования» на 2013—2020 годы (утверждена распоряжением Правительства Российской Федерации от 15 мая 2013 г. № 792-р).

➠ Государственная программа Российской Федерации «Информационное общество (2011—2020 годы)» (утверждена постановлением Правительства Российской Федерации от 15 апреля 2014 г. № 313).

➠ Концепция информационной безопасности детей (утверждена распоряжением Правительства РФ от 2 декабря 2015 г. № 2471-р).

➠ Федеральная целевая программа развития образования на 2016—2020 годы (утверждена постановлением Правительства Российской Федерации от 23 мая 2015 г. № 497 «О Федеральной целевой программе развития образования на 2016—2020 годы»).

➠ Стратегия инновационного развития Российской Федерации на период до 2020 года (утверждена распоряжением Правительства РФ от 08.12.2011 № 2227-р «Об утверждении Стратегии инновационного развития Российской Федерации на период до 2020 года»).

➠ Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).

➠ СанПиН 2.4.2.2821-10 «Гигиенические требования к режиму учебно-воспитательного процесса» (приказ Минздрава от 26.12.2010 № 189).

➠ ГОСТ Р 52872-2012 «Интернет-ресурсы: Требования доступности для инвалидов по зрению».

➠ Приказ Министерства образования и науки РФ от 9 января 2014 года № 2 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

➠ Приказ Министерства образования и науки РФ № 1643 от 29 декабря 2014 года «О внесении изменений в приказ Министерства образования и науки Российской Федерации от 6 октября 2009 г. № 373 “Об утверждении и введении в действие федерального государственного образовательного стандарта начального общего образования”».

➠ Приказ Министерства образования и науки РФ № 1644 от 29 декабря 2014 года «О внесении изменений в приказ Министерства образования и науки Российской Федерации от 17 декабря 2010 г. № 1897 “Об утверждении федерального государственного образовательного стандарта основного общего образования”».

➠ Приказ Министерства образования и науки РФ № 1645 от 29 декабря 2014 года «О внесении изменений в приказ Министерства образования и науки Российской Федерации от 17 мая 2012 г. № 413 “Об утверждении федерального государственного образовательного стандарта среднего (полного) общего образования”».

➠ Приказ Федеральной службы по надзору в сфере образования и науки (Рособрнадзор) № 785 от 29.05.2014 «Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети “Интернет” и формату представления на нем информации».

➠ Постановление Правительства РФ от 10.07.2013 г. № 582 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети “Интернет” и обновления информации об образовательной организации».

Региональный уровень

➠ Приказ Министерства образования Нижегородской об-

ласти «Об утверждении плана реализации государственной программы “Развитие образования Нижегородской области” на 2017 год и плановый период 2018—2019 годов» от 20.01.2017 № 101.

➠ Письмо Министерства образования Нижегородской области «О требованиях к структуре официального сайта образовательной организации» от 08.09.2014 г. № 316-01-100-2751/14.

➠ Письмо Министерства образования Нижегородской области «О профилактике вовлечения детей в противоправные действия через сеть Интернет» от 09.02.2017 г. № 316-01-101-315.

➠ Письмо Министерства образования Нижегородской области «О порядке подачи сообщений о ресурсах в сети Интернет, содержащих запрещенную информацию» от 24.10.2017 г. № 316-01-100-4176/17-00.

Уровень образовательной организации*

➠ Устав образовательной организации.

➠ Программа развития образовательной организации.

➠ Положение об информационном сайте образовательной организации.

➠ Правила использования сети Интернет в образовательной организации.

➠ Положение об электронном обучении.

➠ Приказ об организации обучения с применением электронного обучения и дистанционных образовательных технологий.

➠ Положение об использовании электронной формы учебников.

➠ Положение об электронной библиотеке образовательной организации.

➠ Положение о системе электронного документооборота (СЭД) в образовательной организации. ☺

---

* Приводятся примеры (возможных) нормативных локальных актов образовательной организации.

Программно-технические средства для создания безопасной информационной образовательной среды образовательной организации

Создание безопасной информационной среды для образовательной организации предполагает системный подход в выборе технических средств, а также соблюдение необходимых требований для используемого оборудования и программного обеспечения.

Рассмотрим технические, технологические решения и возможности на примере сервисов и услуг ПАО «Ростелеком». Наличие собственной магистральной сети федерального масштаба, специально оснащенные технологические площадки, надежная и защищенная информационно-коммуникационная инфраструктура, бесперебойное функционирование оборудования и программного обеспечения могут гарантировать предоставление телекоммуникационных услуг высокого качества для образовательной организации.

Контентная фильтрация

Одним из важных аспектов безопасности среды является использование контент-фильтрации.

Безопасность доступа в Интернет для участников образовательного процесса обеспечивается в том числе централизованной системой контентной фильтрации. Система представляет собой программно-аппаратный комплекс, позволяющий централизованно управлять трафиком образовательной организации. Например, система блокирует запрещенные в интернете сайты, причем как отдельные страницы, так и контент внутри страницы, «всплывающие окна», загружаемые на компьютер файлы, обеспечивает поддержку фильтрации текстовых запросов в поисковых системах, производит морфологический анализ страниц, защищает от вредоносных программ, обеспечивает анализ URL запросов и ссылок. При этом система контент-фильтрации определяет категорию пользователя и присвоенную ему политику доступа в сеть

Интернет. Если запрос входит в разрешенную категорию, пользователь сможет получить необходимую информацию, в противном же случае запрос не будет обработан, и для ученика будет отображена информационная страница о «некорректном запросе», который не может быть обслужен.

Обеспечивается возможность гибкой настройки доступа к интернет-ресурсам для различных групп пользователей. Система фильтрации при запросе также сравнивает содержимое сайта с наборами слов и словосочетаний, имеющих пороговый вес, и в том случае, если страница содержит предполагаемый потенциально опасный контент, она направляется на обработку экспертным советом.

Основными типами информации, с которыми работает контент-фильтрация, являются «соцсети и чаты», «наркотики», «азартные игры», «нецензурная лексика», «порнография», «пропаганда экстремизма». Они представлены на рисунке 1.

Услуга контент-фильтрации трафика полностью соответствует требованиям законодательства: ФЗ-436, ФЗ-139, ФЗ-114, Указу Президента РФ № 761 от 1 июня 2012 года, методическим рекомендациям по ограничению в образовательных организациях доступа обучающихся к видам рас-

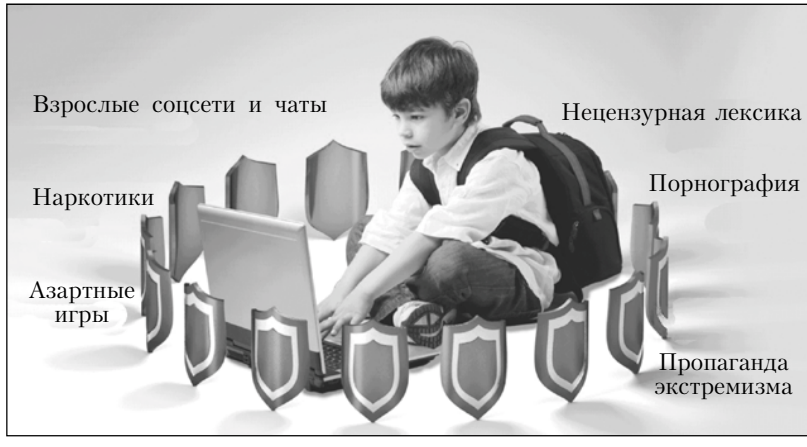


Рис. 1. Основные типы информации для контент-фильтрации

пространяемой в сети Интернет информации, причиняющей вред здоровью или развитию детей. Система успешно прошла испытание на соответствие функциональности и качества фильтрации и уже внедрена в ряде регионов России.

Например, на территории Нижегородской области сервис организован для МБОУ «Школа № 145» и МБОУ «Лицей № 40» (Нижний Новгород), МБОУ «Средняя школа № 2 с углубленным изучением предметов физико-математического цикла» (Дзержинск), МБОУ «Березовская средняя школа» и МБОУ «Новоселковская средняя школа» (Арзамасский район), МБОУ «Средняя школа № 2» (Лысково).

Защищенный доступ в Интернет из виртуальной частной сети

Услуга предоставляет возможность получения прямого защищенного доступа в сеть Интернет из организованной виртуальной частной сети IP VPN (VPN, Virtual Private Network). Виртуальной — поскольку сеть организуется на существующих каналах связи. Частной — потому что сеть принадлежит только организации-заказчику. По сути VPN — это защищенные соединения между локальными сетями, расположенными на расстоянии друг от друга. Услуга VPN позволяет связать все точки организации в единую защищенную корпоративную сеть.

От учебного заведения не требуется организации отдельных линий связи и подключений к системе передачи данных телекоммуникационного оператора. При подключении к VPN обеспечивается полная защищенность ресурсов образовательной организации, входящих в периметр виртуальной частной сети, от сетевых атак и угроз из внешней публичной сети Интернет. При этом образовательной организации предоставляются необходимые инструменты для

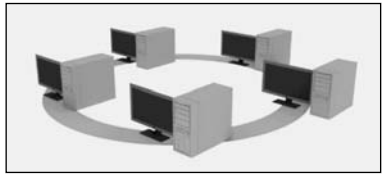


Рис. 2. Схема к VPN

самостоятельного конфигурирования настроек сетевой безопасности.

Услуга оказывается на основании и в соответствии с лицензией № 86475 «Телематические услуги связи», выданной Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации.

Например, услуга VPN организована для проекта «Единая дежурно-диспетчерская служба» в МДОУ «Детский сад № 32 “Росинка”» (Павлово).

Корпоративный внутренний портал

Данный сервис позволяет образовательной организации создать внутренний ресурс, доступный только ее сотрудникам и участникам образовательного процесса.

Функциональные возможности внутреннего портала:

- организация общей области для хранения документов, изображений и другой документации;
- создание списка контактов сотрудников образовательной организации, учащихся;
- создание внутренних сайтов подразделений образовательной организации (классы, кафедры, учебные направления и пр.), сайтов научных групп, что позволяет организовать отдельные области с настраиваемыми правами доступа для хранения документов;
- работа с календарем: создание различных событий и мероприятий, управление событиями и мероприятиями, настраиваемые формы регистрации и рассылка уведомлений;
- удобная система поиска: поиск может производиться как со стартовой страницы портала, так и на уровне сайта подразделения;
- работа с новостями и объявлениями, организация блогов и фотогалерей;
- подключение приложения Microsoft OneDrive for Business для удобной работы с документами и файлами любых типов, хранящихся «в облаке» на портале.

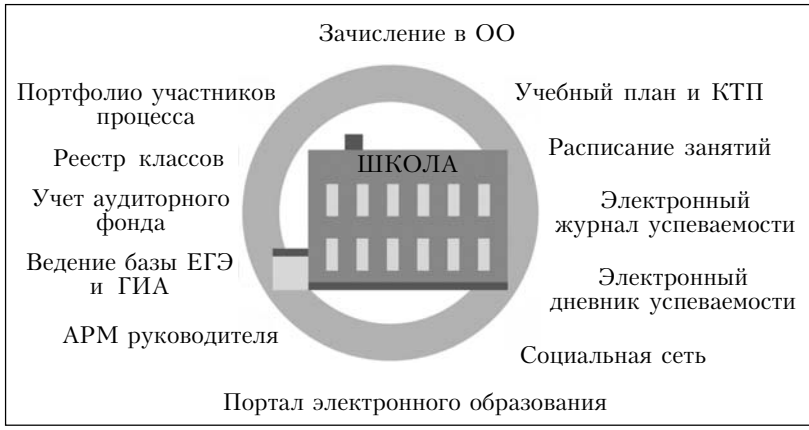


Рис. 3. Основные возможности портала

Возможности корпоративного портала для образовательной организации представлены на рисунке 3.

IP-видеонаблюдение / сервис «Видеокомфорт» в образовательной организации

Видеонаблюдение в образовательной организации призвано обеспечить: взрыво- и пожарную безопасность, антитеррористическую защищенность, экологическую безопасность, безопасность в сфере техники безопасности и охраны труда, предупреждение несчастных случаев и правонарушений.

Основные потребители сервиса: дошкольные образовательные организации, общеобразовательные организации, профессиональные образовательные организации, высшие учебные заведения, организации дополнительного образования, детские оздоровительные организации.

Сервис «Видеокомфорт» в образовательной организации позволяет:

- оперативно реагировать на любую конфликтную ситуацию в стенах организации с ее дальнейшим расследованием;
- не допускать проникновения на территорию образовательной организации и во внутренние помещения зло-

умышленников или посторонних, осуществлять профилактику подобных ситуаций;

- организовать наблюдение за материальными ценностями, оборудованием кабинетов, личными вещами в гардеробе и других местах;
- предупреждать чрезвычайные ситуации и акты вандализма;
- осуществлять профилактику учебной дисциплины, организовывать учет посещаемости учащихся, когда можно точно, до минуты, определить время входа или выхода ребенка из здания.

Организация видеонаблюдения в образовательной организации позволяет использовать следующие возможности сервиса:

- транслировать на интернет-сайте образовательной организации видео в онлайн-режиме;
- формировать видеоархив по событиям;
- использовать мобильные приложения для смартфонов и планшетов;
- предоставлять доступ к видео для сотрудников образовательной организации;
- осуществлять интеграцию с существующими моделями камер, использовать возможность закупки новых универсальных камер;
- использовать видео в работе сотрудников службы безопасности: одновременный вывод нескольких трансляций (до 16) на один экран, быстрый просмотр последних пяти минут на всех камерах, закладки и события, перемотка архива;
- организовывать дистанционное обучение для учеников, в том числе для детей с ограниченными возможностями здоровья;
- формировать сервисы для родителей в части просмотра трансляций на сайте, организовывать дистанционное участие в родительских собраниях;
- интегрироваться с централизованным решением по видеонаблюдению при проведении ЕГЭ.

Для подключения требуются интернет-соединение и IP-видеокамера. Не нужны видеорегистраторы, мониторы и системы хранения данных. Также не требуется организация рабочего места оператора системы, так как все управление видеопотоком происходит через интерфейс, доступный на любых устройствах: компьютере, планшете, мобильном телефоне. Обработка видеопотоков и хранение архива осуществляются на серверах «Ростелекома».

Примеры образовательных организаций, подключивших услугу: МБОУ «Средняя школа № 7 им. Крупнова» (Городец), МДОУ «Детский сад № 3 “Сказка”» (Тоншаево).

Web-видеоконференция для образовательной организации

Услуга «Web-видеоконференция» предоставляет сервис многоточечных видеоконференций, который обеспечивает аудио- и видеосвязь через Интернет без дополнительного оборудования и необходимости аренды студий. Сеансы видеоконференции происходят между географически удаленными друг от друга пользователями через сеть Интернет, при этом пользователи получают возможность видеть и слышать своих собеседников в режиме реального времени.

Услуга «Web-видеоконференции» позволяет дистанционно реализовать совещания, проводить родительские собрания, осуществлять обучение педагогов, учеников и родителей.

Сеансы видеоконференции проходят непосредственно в браузере, на web-странице сервисной платформы. Для обеспечения сеанса видео-конференц-связи используется встроенное в браузер программное обеспечение (плагин), Video Most ActiveX. Необходимое программное обеспечение устанавливается при первом входе в конференцию, а также при обновлении программного обеспечения. Система определяет операционную систему и браузер пользователя и автоматически предлагает установить соответствующий плагин. Схема организации web-видеоконференции представлена на рисунке 4 (с. 19).

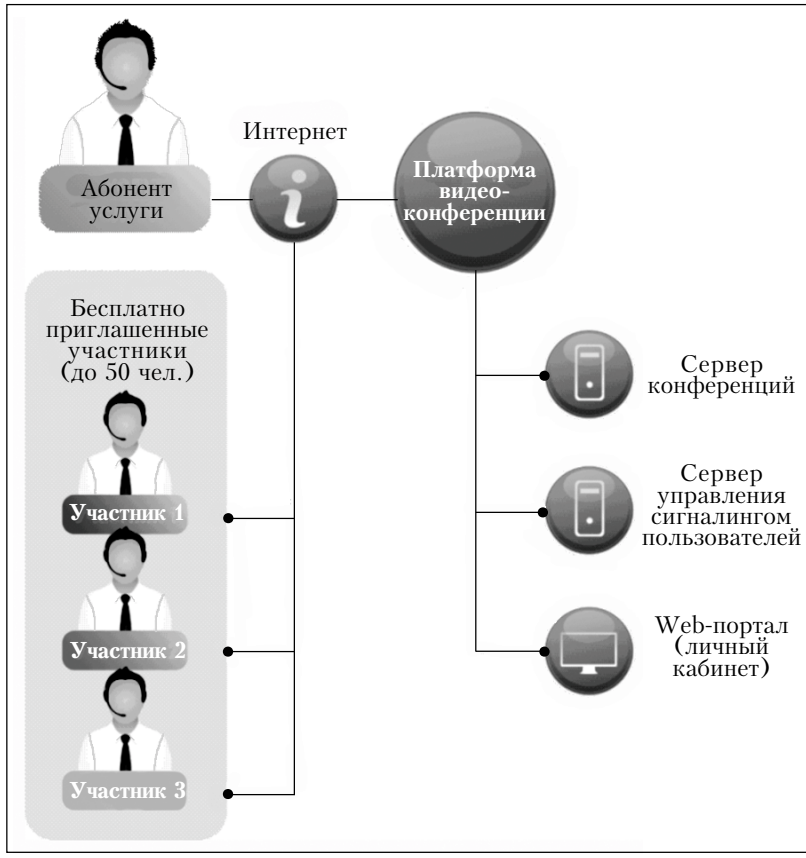


Рис. 4. Схема организации web-видеоконференции

Программная видео-конференц-связь динамически подстраивается к условиям сети. При использовании услуги доступны следующие возможности:

- отправка приглашений пользователям на участие в сеансе web-конференции через почтовый клиент (в виде письма или приглашения на собрание);
- ведение текстового чата между пользователями;
- демонстрация документов, текстовых файлов, таблиц, презентаций и пр. при проведении конференций;
- демонстрация рабочего стола ПК в процессе проведения конференции всем участникам;

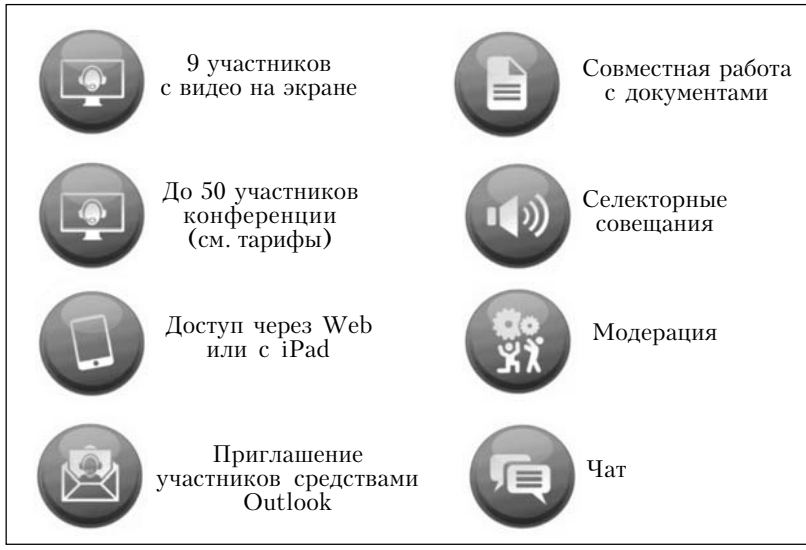


Рис. 5. Основные возможности web-видеоконференции

- возможность обмена файлами при проведении конференции.

Основные возможности web-видеоконференции представлены на рисунке 5.

Для участия в видеоконференции достаточно иметь персональный компьютер, подключенный к сети Интернет, web-камеру, микротелефонную гарнитуру (динамики, микрофон). Интерфейс проведения конференции представлен на рисунке 6.

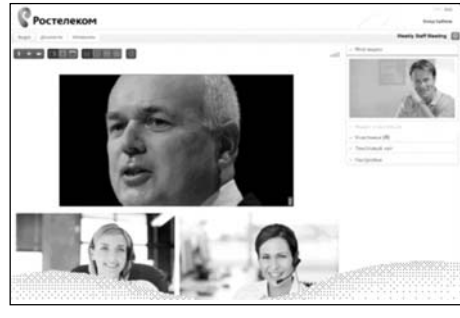


Рис. 6. Интерфейс web-видеоконференции

Рис. 7. Требования к сети

Требования к рабочему месту: компьютер или ноутбук с процессором Intel Core2Duo 2.0 ГГц или выше или iPad, веб-камера с разрешением видео не менее 640 × 480 и частотой кадров не менее 30 Гц.

Требования к камере и микрофону: сервис поддерживает все современные веб-камеры, однако на дешевых / устаревших моделях качество изображения будет невысоким; сервис может работать со встроенным в ноутбук микрофоном, однако для максимального качества желательно использовать гарнитуру.

Требования к сети для организации web-видеоконференции представлены на рисунке 7.

Образовательные организации, использующие услугу «Web-видеоконференция»: МБОУ «Валковская средняя общеобразовательная школа» (Лысково), ГБОУ СПО НО «Краснобаковский лесной колледж» (Красные Баки).

Актуальные аспекты формирования компетенций участников образовательного процесса в сфере создания безопасной информационной образовательной среды

Процессы развития информационного общества оказывают значительное влияние на изменения в системе образования. В настоящее время в образовательных организациях формируется ИОС, которая создает принципиально новые возможности для организации учебной и внеучебной деятельности учащихся. ИОС позволяет выстраивать индивидуально ориентированный процесс обучения, способствует высокой степени самостоятельности и самореализации обучающихся. Доступ к информационным ресурсам интернета дает возможность обучающимся пользоваться основным и дополнительным учебным материалом, необходимым для обучения в школе, выполнять домашние задания, самостоятельно обучаться.

В последние годы аудитория интернет-пользователей стремительно растет. Ее значительную часть составляет молодое поколение. Дети и подростки открывают для себя мир посредством интернета.

Необходимо отметить, что две трети учащихся выходят в Глобальную сеть самостоятельно, без присмотра родителей и педагогов. Многие школьники посещают веб-страницы нежелательного и запрещенного содержания. Бесконтрольный доступ к интернету может привести к негативным последствиям. В интернете существуют самые разнообразные угрозы, и дети, выходящие в сеть самостоятельно, безусловно, являются объектом, на который эти угрозы направлены.

В числе опасностей, ожидающих детей и подростков в интернете, прежде всего следует выделить сайты, представляющие угрозу для жизни и здоровья детей; сайты, содержащие контент для взрослых; сайты, разжигающие национальную рознь и расовое неприятие, пропагандирующие жестокость, насилие; сайты сект, знакомств и т. д.

Кроме того, в подростковой среде появились такие от-

клонения, как компьютерная и интернет-зависимость, игромания, кибербуллинг (травля в интернете).

Таким образом, использование сети Интернет может иметь нежелательные последствия для любого неумелого пользователя, к которым прежде всего относятся дети школьного возраста. Следовательно, школа должна обеспечить для них безопасную информационную среду и привить необходимые навыки безопасного использования сети Интернет, а также научить родителей создавать подобную среду дома.

Сегодня существует достаточно широкий спектр программных средств, позволяющих ограничить доступ детей к интернет-сайтам с негативным содержанием, однако только техническими средствами проблему не решить. Согласно исследованиям, пока еще нет компьютерных программ, способных полностью защитить пользователя от доступа к нежелательной информации. Даже лучшие программные продукты не способны полностью отсечь потенциально опасный контент. Самым эффективным механизмом обеспечения информационной безопасности несовершеннолетних может и должно стать формирование информационной культуры детей и родителей, а также профессиональной информационной культуры педагогов.

По мнению специалистов, занимающихся вопросами безопасности детей в интернете, лучший фильтр, который может обеспечить безопасность ребенка в сети и решить многие другие проблемы, — в голове самого ребенка, а взрослым нужно только «настроить» этот фильтр.

Иными словами, важным направлением деятельности образовательной организации должны стать формирование у несовершеннолетних навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде, готовности и способности регулировать информационные опасности вокруг себя, развитие способности распознавать негативную информацию в интернет-пространстве и противостоять ей. Задача формирования у современного подростка навыков и умений позитивного и полезного взаимодействия с информационной средой долж-

на решаться как на уроке, так и во внеурочной деятельности.

Единое информационное пространство образовательной организации — это система, в которой задействованы и на информационном уровне связаны все участники образовательного процесса: администрация — учитель — ученик — родитель, — поэтому обеспечение безопасности при использовании компьютера и интернета детьми требует комплексного подхода.

Комплексный подход к решению проблемы информационной безопасности в образовательной организации выражается в планомерной реализации программы формирования БИОС. БИОС предполагает построение и воплощение в жизнь социально-педагогической модели профилактической деятельности с целью оздоровления социальной среды, окружающей ребенка, и осуществления ряда защитных функций, направленных на предотвращение воздействия информационных угроз и различных видов информационной зависимости среди детей и молодежи.

Целью программы построения БИОС является создание тщательно спроектированного образовательно-воспитательного пространства образовательной организации, включающего комплекс мероприятий, вовлекающих всех участников образовательного процесса (учащихся всех возрастных категорий, педагогов и родителей) в формирование БИОС.

Программа может быть самостоятельной или входить как модуль в программу развития образовательной организации.

Программа должна включать комплекс учебно-просветительских мероприятий для учащихся, педагогов, родителей, а также создание и развитие информационных ресурсов, предполагающих информирование о видах интернет-угроз и способах противодействия им.

Работа в данном направлении в первую очередь должна начинаться на уроках информатики. В программу курса информатики в 5—11-х классах должны быть включены уроки по грамотному и безопасному использованию сети Интернет. В начальных классах также необходимо проводить

пропедевтические мероприятия по данной тематике, например в рамках классных часов.

Для безопасного пользования интернетом учащиеся должны знать ряд правил:

➠ Никогда не предоставлять частную информацию о себе (фамилию, номер телефона, адрес, номер школы) без разрешения родителей. Для регистрации лучше не использовать свое имя, а придумать ник.

➠ Всегда быть вежливыми в электронной переписке, и ваши корреспонденты будут вежливыми с вами.

➠ При обнаружении чего-либо, смущающего вас, при разговоре со сверстниками или взрослыми людьми, переписке или получении рассылок по электронной почте, самостоятельном обнаружении в сети, не стараться разобраться в этом самим, а обратиться к родителям или учителям — они знают, что надо делать.

➠ Для регистрации необходимо придумать сложный пароль (содержащий не только буквы, но и цифры) и никому не давать свой пароль, за исключением взрослых вашей семьи.

➠ Не совершать покупки в интернете без совета взрослых.

➠ Не переходить по подозрительным ссылкам, которые присылают вам в социальных сетях.

➠ Не ходить на встречи с новыми знакомыми из сети Интернет, не предупредив взрослых и без их разрешения.

➠ При использовании чужих компьютеров не забывать выходить из своих профилей, иначе следующий пользователь может просмотреть вашу личную информацию.

➠ Быть терпимым к недостаткам окружающих вас людей! Не смотреть на то, соблюдают или нет ваши собеседники правила сетевого этикета, — соблюдать их самим!

Необходимо учитывать, что время использования интернета для различных возрастов должно быть ограничено:

➠ 5—7 лет — от 15 минут до получаса в день;

➠ 7—12 лет — не более 1 часа;

➠ 12—16 лет — около 2 часов.

Для обучения школьников безопасному использованию сети Интернет могут применяться такие интерактивные интернет-ресурсы, как:

- «Мультимедийный учебный дистанционный курс безопасного пользования ресурсами сети Интернет»: https://onlinesafety.info/;
- онлайн-курс «Понятный Интернет»: http://zaprosto-internet.ru/GOOGLE_BOOK_PRINT.pdf;
- материалы интернет-портала «Дружественный Рунет»: http://www.friendlyrunet.ru/;
- материалы интернет-портала «Что ты знаешь о защите персональных данных»: персональныеданные.дети (http://xn—80aalcbc2bocdadlpp9nfk.xn—d1acj3b/);
- энциклопедия безопасности на веб-сайте Лиги безопасного Интернета: http://ligainternet.ru/encyclopedia-of-security/;
- Энциклопедия «Все об угрозах, вирусах и спаме» на сайте Лаборатории Касперского: https://securelist.ru/enciklopediya/;
- онлайн-тест и онлайн-игра на портале «Разбираем Интернет»: http://www.razbiraeminternet.ru/;
- онлайн-тест на киберграмотность Лаборатории Касперского: http://www.kaspersky.ru/about/news/virus/2015/cybergrammar;
- онлайн-тест в информационном разделе сети образовательных организаций Ярославской области: http://www.edu.yar.ru/safety/testing.html;
- ресурсы веб-сайта «Сетевичок»: сетевичок.рф (http://xn—b1afankxqj2c.xn—p1ai/).

Во внеурочную деятельность также должны быть включены мероприятия не только профилактического и обучающего характера, но и демонстрирующие учащимся информационные, образовательные и развивающие возможности сети Интернет.

Примеры таких мероприятий:

- Неделя безопасного интернета;
- творческие конкурсы для разных возрастных групп:

«Сказка о золотых правилах безопасности в интернете», «Информация: важная, полезная, опасная, вредная», «Основы информационной безопасности», «Правила поведения в сети Интернет», «Компьютер и интернет — друзья, враги, помощники?»;

➠ участие в образовательных онлайн-мероприятиях: олимпиадах, проектах, акциях, флешмобах.

Задача системы образования — формирование личности, не только психологически устойчивой к негативным информационным воздействиям социальной среды, но и владеющей умениями ее конструктивного преобразования. Поэтому важным аспектом формирования БИОС является организация занятости детей и подростков социально значимой деятельностью. Ребенок, вовлеченный в интересное дело, воспитанный в духе гражданственности, патриотизма, толерантности, сориентированный на общечеловеческие ценности, сумеет противостоять негативному влиянию современной информационной среды и определить для себя правильную линию поведения и жизнедеятельности.

Важной составной частью программы должны стать мероприятия, вовлекающие учащихся в созидательную сетевую деятельность, дающую положительный опыт сетевого взаимодействия, в частности в проектную деятельность в сети Интернет и другие сетевые активности.

Работа по обеспечению информационной безопасности детей и подростков не принесет результатов без повышения компетентности в этом вопросе родителей, которые зачастую отстают от информационной грамотности своего ребенка и не подозревают, какой опасности он подвергается, сидя бесконтрольно дома за компьютером. Некоторые родители считают, что ненормированное «сидение» ребенка в сети лучше, чем прогулки в сомнительных компаниях. Родители, с ранних лет обучая ребенка основам безопасности дома и на улице, между тем, «выпуская» его в интернет, не представляют себе, что точно так же нужно обучить его основам безопасности в сети. В связи с этим необходимо информировать родителей о видах информации, способной причинить вред

здоровью и развитию несовершеннолетних, и о правилах безопасного поведения в сети Интернет.

Тематика проведения различных мероприятий с родителями может быть самой разнообразной, например:

- Правильная организация работы с компьютером.
- Виды интернет-угроз.
- Вирусы и средства борьбы с ними.
- Технические средства защиты информации.
- Безопасная работа в интернете: анализ веб-сайтов, безопасный поиск, надежные пароли.
- Компьютерные вирусы и методы борьбы с ними.
- Антивирусные программы, установка, настройка и работа с ними.
- Программы родительского контроля.
- Противозаконная, неэтичная и вредоносная информация в интернете: как ее избежать.
- Достоверность информации в интернете, проблемы и способы проверки информации на достоверность и полноту.
- Этика сетевого общения.
- Личная информация: нужна ли она в интернете, как защитить личную информацию в блогах, социальных сетях и пр.
- Социальные сети: как общаться в сети и не попасть в сети мошенников и злоумышленников.
- Что такое хакерство.
- Интернет-зависимость: угрозы, реальность, проблемы, решения.
- Web-серфинг: как не потерять себя и свое время в интернете.
- Как распознать кибермошенничество и не стать его жертвой.
- Предложения в электронных письмах и как не попасться на удочку мошенников.
- Что такое киберхулиганство: как не стать жертвой киберхулиганов.
- Как защитить свою почту от спама и не стать невольно спамером.

➠ Киберпреступления в законодательстве России.

➠ Безопасность в коммерческих интернет-сервисах: интернет-магазины, услуги различных фирм и др.

➠ Компьютерные игры, как не стать игроманом, азартные игры в интернете.

➠ Мобильные угрозы в современном мире.

➠ Как правильно вести себя с киберхулиганами и защититься от нежелательного общения.

Большое значение для эффективности мероприятия имеет не только содержание, но и форма его проведения.

Целесообразно использовать следующие формы работы с родителями:

➠ тематические родительские собрания;

➠ беседы, семинары, круглые столы, тренинги, пресс-конференции, занятия-практикумы, деловые игры, дискуссии;

➠ лекции, встречи со специалистами, системными администраторами;

➠ реализация программы психолого-педагогического просвещения родителей (родительский всеобуч);

➠ вовлечение родителей в сетевое взаимодействие (сайты школ, блоги педагогов и руководителей);

➠ информирование:

— информационные панели, стенды;

— специальный раздел на сайте образовательной организации;

— подготовка печатной продукции: памятки для родителей, буклеты, информационные бюллетени, специальные выпуски школьных газет.

До сведения родителей необходимо довести информацию о линиях помощи детям и их родителям в случаях интернет-угроз, действующих в России.

В настоящее время в России действуют три линии помощи:

➠ на сайте «Дети онлайн»: http://detionline.com/;

➠ на сайте Центра безопасного Интернета в России: http://www.saferunet.org/;

➠ на сайте «Не допусти!»: http://nedopusti.ru/.

Что необходимо знать взрослым об опасностях интернета

Для обеспечения безопасности детей в сети Интернет и собственной безопасности следует знать виды интернет-угроз, уметь распознавать и предотвращать их. Для этого нужно рассказать детям о виртуальном мире, его возможностях и опасностях как можно больше. Необходимо проанализировать и затем вместе с детьми изучить интересные и полезные интернет-ресурсы по безопасному поведению в сети Интернет. Следует научить детей и родителей, как реагировать в случае, если их кто-то обидел или они получили / натолкнулись на нежелательный и агрессивный контент в интернете, рассказать, куда в подобном случае они могут обратиться.

При проведении бесед для родителей детей *младшего школьного возраста* рекомендуется использовать материалы, размещенные:

- на сайте интерактивного курса по интернет-безопасности (http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/etusivu.htm) в разделе «Для учащихся» — рассказы для детей 7—10 лет, а также в разделе «Тесты» (можно организовать online-тестирование школьников 7—10 лет);
- на сайте «On-ляндия. Безопасная веб-страна» (http://www.onlandia.org.ua/ru-RU/) в разделе «Для детей 7—10 лет» — рассказы в картинках, задания и вопросы;
- на сайте информационно-аналитического ресурса «Ваш личный Интернет» (http://content-filtering.ru/aboutus/) в разделе «Юным пользователям», подраздел «Дошкольники и младшие классы» — подсказки и советы по безопасному поведению в сети Интернет;
- на сайте федерального проекта по борьбе с мобильным мошенничеством компании «МегаФон» (http://stopfraud.megafon.ru/) в разделах «Виды мошенничества» и «Наши рекомендации», а также советы родителям;
- на портале «Безопасный Интернет» (http://www.saferinternet.ru/) законодательство в сфере информацион-

ной безопасности и другие разделы, содержащие материалы по теме «Безопасный интернет»;

➠ в качестве видеозаставки для беседы можно использовать мультфильм «Безопасный Интернет», который разработала студия Mozga.ru, на сайте «Началка.ком» материалы по безопасному интернету (http://www.nachalka.com/taxonomy/term/335).

При проведении собраний для родителей *учащихся 11—14 лет* целесообразно использовать материалы, размещенные:

➠ на сайте интерактивного курса по интернет-безопасности (http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/etusivu.htm) в разделе «Для учащихся» — рассказы для детей 11—16 лет, а также в разделе «Тесты» (можно организовать online-тестирование учащихся 11—14 лет);

➠ на сайте «On-ляндия. Безопасная веб-страна» (http://www.onlandia.org.ua/ru-RU/) в разделе «Для детей 11—14 лет» — рассказы в картинках, задания и вопросы; в разделе «Для учителей» — опасности и поведение в сети;

➠ на сайте информационно-аналитического ресурса «Ваш личный Интернет» в разделе «Юным пользователям», «Средние классы» — подсказки и советы по безопасному поведению в сети Интернет, а также при использовании онлайн-игр и мобильного телефона;

➠ на сайте федерального проекта по борьбе с мобильным мошенничеством компании «МегаФон» (http://stopfraud.megafon.ru/) в разделах «Виды мошенничества» и «Наши рекомендации», а также советы родителям;

➠ на портале «Безопасный Интернет» (http://www.saferinternet.ru/) — законодательство в сфере информационной безопасности и другие разделы, содержащие материалы по теме «Безопасный интернет».

При проведении занятий и мероприятий со *старшеклассниками* рекомендуется использовать материалы, размещенные:

➠ на сайте интерактивного курса по интернет-безопас-

ности (http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/etusivu. htm) в разделе «Для учащихся» — рассказы для детей 11—16 лет, а также в разделе «Тесты» (можно организовать online-тестирование школьников 11—14 лет);

- на сайте «On-ляндия. Безопасная веб-страна» (http://www.onlandia.org.ua/ru-RU/) в разделе «Для подростков» — советы по безопасному общению и работе в режиме online; в разделе «Для учителей» — опасности и поведение в сети;
- на сайте информационно-аналитического ресурса «Ваш личный Интернет» (http://content-filtering.ru/aboutus/) в разделе «Юным пользователям», подраздел «Старшие классы» — подсказки и советы по безопасному поведению в сети Интернет, а также при использовании онлайн-игр и мобильного телефона;
- на сайте федерального проекта по борьбе с мобильным мошенничеством компании «МегаФон» (http://stopfraud.megafon.ru/) в разделах «Виды мошенничества» и «Наши рекомендации», а также советы родителям;
- на портале «Безопасный Интернет» (http://www.saferinternet.ru/) — законодательство в сфере информационной безопасности и другие разделы, содержащие материалы по теме «Безопасный интернет».

Большая часть работы по обеспечению информационной безопасности детей — это работа с педагогами, осуществляющими профессиональную деятельность в условиях широкого внедрения средств информационных и коммуникационных технологий в образовательное пространство школы.

Учитель способен подготовить сознание детей к противодействию негативным информационным влияниям, формировать информационную грамотность (навыки критического мышления), развивать способности к самоблокированию информации, учить отличать качественную информацию от некачественной. Поэтому педагог должен обладать необходимыми компетенциями в сфере информационной безопас-

ности детей и молодежи, которые он может приобрести в ходе освоения дополнительных профессиональных программ. Так, на кафедре информационных технологий ГБОУ ДПО НИРО уже несколько лет в дистанционном формате реализуется программа «Современные подходы к обеспечению безопасной работы детей в сети Интернет». Тема, посвященная информационной безопасности детей и молодежи, включена в ряд учебных курсов.

Однако работа с учителями не должна ограничиваться однократным повышением квалификации, она должна проводиться систематически. Таким образом, возникает необходимость в разработке специальных занятий для педагогов, включающих теоретические семинары и практические занятия по теме «Информационная безопасность школьника».

Отдельные вопросы информационной безопасности школьников целесообразно рассматривать в рамках педагогических советов и заседаний школьных и районных методических объединений.

В содержание материалов, осваиваемых педагогами, должны быть включены следующие основные компоненты и темы:

- Основные понятия информационной безопасности.
- Правовые основы информационной безопасности и защита конфиденциальной информации.
- Информационная безопасность субъектов образовательного процесса.
- Угрозы информационно-психологической безопасности личности и их основные источники.
- Виды информационных угроз.
- Программные средства защиты персональной информации.
- Технические средства защиты и комплексное обеспечение информационной безопасности.
- Безопасность в сети Интернет.
- Правила и нормы сетевого этикета.
- Виды отклоняющегося, зависимого поведения школьников и методы их предупреждения и устранения.

➠ Санитарные нормы и правила работы за компьютером.

Большая роль в профилактической работе с учащимися отводится педагогу-психологу, который в течение учебного года должен проводить индивидуальную работу с обучающимися (по запросу родителей) и групповую работу по теме интернет-зависимости в соответствии с планом реализации программы первичной профилактики компьютерной и игровой зависимости среди несовершеннолетних; выступать на общешкольном и классных родительских собраниях на тему «Интернет в жизни вашего ребенка», вести профилактическую работу с родителями.

Отметим также, что сегодня Интернет является важной составляющей информационных ресурсов современной библиотеки. Библиотека в дополнение к печатным ресурсам предоставляет доступ к электронным информационным ресурсам и, что немаловажно, помогает ориентироваться в них.

Библиотекари, работающие с детьми, — это просветители и консультанты по безопасности в интернете, а также «лоцманы-навигаторы» в киберпространстве.

Библиотекари могут:

➠ рассказать детям и родителям об опасностях интернета;

➠ предоставить родителям информацию о способах защиты детей от интернет-угроз;

➠ обучить детей различным умениям работы с информацией;

➠ помочь в «навигации» по информационным сетям;

➠ рассказать о лучших ресурсах для детей;

➠ организовать тематические мероприятия, конкурсы;

➠ создавать безопасные «детские» интернет-ресурсы.

В образовательной организации должна осуществляться системная работа по информированию учащихся, педагогов и родителей в сфере грамотного и безопасного использования сети Интернет. Такая работа может проводиться в нескольких направлениях.

В информационном образовательном пространстве обра-

зовательной организации должны регулярно в течение года оформляться школьные стенды, классные уголки, распространяться памятки, информационные листки, буклеты, на которых размещается актуальная информация по данной тематике, предназначенная для определенной целевой аудитории (учащихся, педагогов, родителей). Важная роль для продвижения информации в этом направлении отводится школьной газете (журналу), где статьи по информационной безопасности должны занимать видное место, быть периодическими, освещать различные аспекты проблемы безопасности в сети Интернет, отражать текущее состояние проблемы в школе и ставить задачи для ее решения в будущем.

На сайте образовательной организации должна быть специальная страница, на которой размещаются ссылки на полезные ресурсы и актуальные материалы, информирующие всех участников образовательного процесса о правилах безопасного поведения в сети Интернет.

В локальной сети образовательной организации, в медиатеке (библиотеке) образовательной организации должна быть создана и пополняться копилка материалов и методических разработок по безопасности в информационной образовательной среде.

В деятельности школьных творческих объединений, таких, например, как видеостудия, тема БИОС может стать основой для создания творческих проектов.

Технология создания видеофильмов по определенной тематике — это эффективный инструмент в руках педагога. Развитие возможностей цифровой обработки информации значительно расширяет возможности создания видеофильмов для пользователей (педагогов, обучающихся, родителей). Разнообразные устройства для видеосъемки, программное обеспечение для редактирования, конвертирования, вывода видеофайлов и пр. позволяют сделать этот процесс интуитивно понятным, быстрым в освоении и не затратным по времени при создании готового продукта.

Практической реализацией полученных педагогами зна-

ний и умений при работе с видео является внедрение данных технологий в образовательный процесс, что создает ряд преимуществ.

➠ Готовые видеофильмы, созданные по конкретной теме, в данном случае «Безопасность детей в интернете», и предоставляющие связанную с этой темой информацию, могут стать учебными пособиями и использоваться как на уроках, так и при проведении различных образовательных мероприятий.

➠ Процесс создания видеофильмов превращается для участников в образовательное мероприятие, так как требует выполнения алгоритма работы с информацией от замысла до готового продукта через стадии обработки информации, что само по себе является увлекательным и познавательным действом для педагогов и учащихся. При этом следует отметить, что дети в этом процессе переходят от роли потребителей образовательных продуктов к роли их созидателей, гораздо эффективнее усваивая необходимую информацию, приобретая чувство ответственности за нее. В такой деятельности формируются навыки проектирования, работы в группе, творческой деятельности и т. д., что делает процесс обучения интересным и притягательным.

➠ Разнообразие жанров создаваемого видео помогает педагогам сформировать у детей навыки, присущие той или иной специальности: при создании новостных видеофильмов — корреспондента и ведущего, телеоператора; при создании анимационных фильмов — аниматора, дизайнера, художника; и т. д. Независимо от жанра видеофильма дети получают навыки обработки цифровых видеоматериалов, видео- и фотосъемки, работы со звуком и текстом.

➠ Педагоги в реальности получают платформу для реализации своей роли в учебном процессе как роли учителя — его организатора, консультанта. Существующие технологии позволяют, например, использовать запись с экрана дисплея (скринвидео), тем самым предоставляя педагогу возможность быстро создать учебный фильм, в котором учащимся будут продемонстрированы те или иные веб-страни-

цы в Интернете, необходимые в учебном процессе, даны комментарии для их использования, поставлены учебные вопросы и т. д.

➠ Создание видео — это технология творчества. Например, при создании видеофильмов по технологии Stop Motion используются совершенно разные материалы: пластилин, цветные карандаши и бумага, конструктор лего, фрукты, игрушки, экран монитора в качестве фона для съемки и т. д., — что превращает работу с видео в увлекательную игру.

➠ Организация видеостудии — это развитие технического и технологического обеспечения образовательных организаций, приобретение и использование соответствующих средств и программного обеспечения для данного вида деятельности.

Таким образом, только при объединении усилий всех участников образовательного процесса возможны создание и эффективное функционирование системы безопасной информационной среды для детей в их образовательной деятельности. ☺

МЕТОДИЧЕСКИЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Эффективный опыт развития безопасной информационной образовательной среды образовательной организации

Для формирования у подрастающего поколения навыков грамотного, безопасного и ответственного поведения в сети Интернет, повышения ИКТ-компетентности педагогов, учащихся и их родителей Нижегородский институт развития образования и макрорегиональный филиал «Волга» ПАО «Ростелеком» провели в 2016 году *конкурс «Безопасная информационная образовательная среда образовательной организации»*. Участники конкурса предоставили проекты, позволяющие оценить опыт образовательной организации по созданию безопасной информационной образовательной среды. В конкурсе принимали участие образовательные организации Нижнего Новгорода и Нижегородской области. Конкурс был поддержан Министерством информационных технологий, связи и средств массовой информации Нижегородской области, ГАУ НО «Редакция газеты “Земля Нижегородская”».

Конкурс показал, что школы в своей деятельности опираются на совместные усилия учителей, родителей и самих школьников и осуществляют меры по обеспечению личной

информационной среды школьников в рамках направлений: программно-технического, организационно-управленческого, научно-методического.

По итогам конкурса *гран-при* был присужден МБОУ «Школа № 105» Нижнего Новгорода (директор И. Н. Мулянова, автор проекта Е. А. Маслова). Проект данной образовательной организации — «Безопасная информационная образовательная среда МБОУ “Школа № 105”» — в наибольшей степени отражает системный подход к решению задач обеспечения безопасной информационной образовательной среды образовательной организации (см. рис. 8 на с. 40).

Материально-техническая база школы позволила всем участникам образовательного процесса работать в едином информационном образовательном пространстве. Все кабинеты оснащены компьютерной техникой и имеют выход в интернет. В школе работают сервер и локальная сеть. Учителя и обучающиеся используют интернет не только во время уроков, но и во внеурочной деятельности, активно участвуют в сетевых проектах, интернет-конкурсах и олимпиадах. Для создания безопасной информационно-образовательной среды задействованы все ресурсы и возможные средства: материальные, технические, кадровые, образовательные, информационные и т. д.

Для организации технического контроля по обеспечению безопасной информационной образовательной среды в школе на все компьютеры установлена лицензионная антивирусная программа Лаборатории Касперского и для контроля интернет-доступа — сетевой фильтр «NetPolice», контент-фильтрация от ЗАО «ЭР-Телеком Холдинг».

На основании федеральных и региональных законов создана программа безопасного поведения обучающихся в сети Интернет «Безопасный интернет», разработан план реализации программы, утверждены локальные акты, регламентирующие основные положения, этапы, цели, задачи и правила проведения проекта. В приложении 1 приведен годовой план мероприятий по теме «Безопасный интернет».

Рис. 8. Схема организации безопасной информационной образовательной среды в школе

Для обеспечения психологической безопасности несовершеннолетних обучающихся на педагогическом совете принята «Программа первичной профилактики компьютерной и интернет-зависимости», в соответствии с которой педагогом-психологом создан «План работы педагога-психолога по реализации программы первичной профилактики компьютерной и игровой зависимости среди несовершеннолетних» (Приложение 2).

Образовательно-методический комплекс по организации безопасной информационной образовательной среды для эффективного процесса обучения и воспитания обучающихся реализуется на трех уровнях: работа с обучающимися; работа с родителями; информационные ресурсы.

Деятельность в данном направлении начинается на уроках информатики. Обучающиеся знакомятся с правилами безопасной работы в сети Интернет, проходят интерактивные тесты по правилам безопасного поведения в сети Интернет (Приложение 3). В каждом учебном кабинете ведется журнал учета работы в сети Интернет, где фиксируются дата, время и цель выхода в интернет.

Педагоги разрабатывают и регулярно проводят с обучающимися классные часы и внеурочные мероприятия (Приложение 4), с родителями — тематические родительские собрания по теме «Безопасность в сети Интернет» (Приложения 5, 6, 7, 8).

Педагог-психолог в течение учебного года ведет индивидуальную работу с обучающимися по запросу родителей и групповую работу по теме интернет-зависимости, выступает на общешкольном родительском собрании на тему «Интернет в жизни вашего ребенка», осуществляет профилактическую работу с родителями. Формы взаимодействия с родителями различны — родительские собрания, индивидуальные беседы, лекции, брошюры «Как избежать интернет-зависимости ребенка» и пр.

В школе действует творческая группа «Юниор-тьютор “ЮнитиК”», важной задачей которой является информирование обучающихся младших классов о безопасном поведе-

нии в сети Интернет. Для учащихся начальных классов участники группы разрабатывают и показывают инсценированные представления, в которых герои мультфильмов доступно и интересно рассказывают детям о правильном поведении в сети Интернет, вручают буклеты (Приложение 9).

Ученики школы активно участвуют в конкурсах и мероприятиях разного уровня, связанных с темой безопасности в информационной образовательной среде, — онлайн-квесте «Сетевичок», едином уроке безопасности школьников в сети Интернет, образовательной акции «Час кода», районных и школьных интерактивных конкурсах, посвященных теме «Безопасный интернет».

В целях информирования обучающихся по вопросам безопасности в информационном образовательном пространстве регулярно в течение года оформляются школьные стенды, классные уголки, распространяются памятки, листовки, буклеты. На сайте школы создана специальная страница, на которой размещаются материалы, призывающие к безопасному поведению в сети Интернет. Важным информационным ресурсом является школьная газета «Стопятка».

Большое внимание уделяется подготовке кадровых ресурсов. Обучение педагогов в школе происходит посредством обмена опытом в рамках мастер-классов, круглых столов, педсоветов и т. д. В образовательной организации накоплено достаточно много методических материалов по теме безопасности, в локальной сети создана и постоянно пополняется копилка методических разработок учителей.

Активно осуществляется сотрудничество с внешними партнерами. Так, при поддержке компании «Ростелеком» в школе прошло большое мероприятие под названием «Сокровища и тайны Интернет-океана», на котором ученики и их родители узнали о различных мерах безопасности в сети Интернет.

Системный подход к решению задач обеспечения безопасной информационной образовательной среды обеспечил успех образовательной организации в этом направлении.

В *номинации «Программно-техническое решение для обеспечения безопасной информационной образовательной среды образовательной организации»* были представлены модели использования различных аппаратных и программных средств, программных средств защиты информации (сетевых фильтров, антивирусных программ и др.). Победителями и призерами стали МБОУ «Водоватовская СШ» Арзамасского района (1-е место), МБОУ «Воротынская СШ» (2-е место), МАОУ «СШ № 151 с углубленным изучением отдельных предметов» Нижнего Новгорода (3-е место).

Фильтрация контента в школе сегодня является актуальной проблемой, которая до сих пор в некоторых образовательных организациях является либо нерешенной, либо решенной крайне неэффективно. Сам процесс фильтрации информации весьма противоречив, тем не менее детей необходимо ограждать от нежелательного контента в сети Интернет. Анализ большинства программ показал, что данная задача может успешно решаться как средствами бесплатного программного обеспечения, так и с привлечением платных услуг.

В проекте МБОУ «Водоватовская СШ» Арзамасского района «Бесплатный контент-фильтр для школы» (автор С. И. Галкин) предложен вариант бесплатной системы контентной фильтрации, который работает независимо от типа клиентской операционной системы. Фильтрация контента установлена на один компьютер (сервер), браузеры всех остальных компьютеров обращаются к нему.

Существует несколько подходов к фильтрации контента: «белый список», «черный список», фильтрация по фразам, фильтрация с помощью фильтрующих DNS-серверов. Каждый из этих способов имеет как достоинства, так и недостатки.

Тип фильтрации «белый список» представляет собой фильтрацию по принципу «запрещено все, что не разрешено», то есть можно посещать только сайты, чьи адреса перечислены. Данный тип фильтрации способен полностью исключить возможность появления на мониторах учащихся

информации, не совместимой с задачами образования, к тому же это самый надежный вариант для защиты детей от неправомерного контента и при этом самый неудобный для поиска информации. Привычный поиск с помощью поисковых систем практически невозможен, «белый список» обязательно должен сопровождаться каталогом ресурсов. Фильтрацию по «белому списку» можно реализовать в Dansguardian, причем без привязки к IP-адресу компьютера. Степень фильтрации контента зависит не от рабочего места, а от логина, который введен пользователем. За одним компьютером может работать и учитель, и учащийся, и администратор, и для каждого из пользователей будет применяться своя степень фильтрации, причем безо всякой предварительной перенастройки.

Вариант фильтрации «черный список» — это список сайтов, доступ к которым будет запрещен. «Черный список» неэффективен, так как в сутки появляются сотни «нехороших» сайтов. Однако в некоторых случаях этот тип фильтрации удобно использовать для фильтрации поисковых запросов и блокировки социальных сетей и фотогалерей поисковых систем. Для реализации фильтрации по типу «черный список» используется программа Rejik (Redirector).

Третий тип — «фильтрация по фразам» — самый сложный и самый эффективный. Суть его заключается в анализе страниц сайтов. Если на странице содержатся «запрещенные» слова, то эта страница блокируется и ее содержание на экране не появится. Прежде чем эта защита заработает, придется ввести все «нехорошие» фразы в специальный список. Кроме того, это самый медленный тип фильтрации: пока содержание страницы не будет проанализировано, не будет видно ни саму страницу, ни сообщения о ее блокировке. Процесс можно ускорить, используя «черный список». Для блокировки с его помощью требуется только адрес сайта, а не анализ всего содержимого страницы. Фильтрация по фразам осуществляется с помощью программы Dansguardian.

Еще один тип фильтрации — фильтрация с помощью фильтрующих DNS-серверов. Принцип их работы основан на отправке пользователем стороннему серверу запроса на разрешение IP-адреса ресурса. Адрес ресурса проверяется по базе данных запрещенных имен, и в случае его нахождения там пользователю возвращается адрес страницы блокировки. Фактически этот вариант представляет уже описанный «черный список», с той лишь разницей, что список составляется компанией, услугами которой пользуется образовательная организация. В школе апробирована работа пяти DNS-серверов: публичного DNS-сервера Google, OpenDNS, SkyDNS, Яндекс.DNS и Norton ConnectSafe. Самую жесткую и эффективную фильтрацию осуществляет SkyDNS.

Поскольку ни один из вариантов не дает надежного, легкого и бесплатного способа решения проблемы контент-фильтрации, в школьной системе фильтрации используются все перечисленные варианты на сервере, что позволяет максимально обезопасить сеть Интернет.

Система полноценно работает на компьютерах как с ОС Windows, так и с ОС Linux. Решается круг сопутствующих проблем: как организовать сетевое хранилище, как предусмотреть возможность централизованной раздачи учебного материала, как организовать централизованное обновление антивирусных баз на рабочих местах под управлением операционной системы Windows. Школьный сервер Водоватовской школы работает под управлением операционной системы AltLinux Школьный сервер 5.02. Настройка и коррекция осуществляются только на сервере, что исключает необходимость в настройке на каждой рабочей станции. Подобная система обслуживает около 40 рабочих мест учащихся, преподавателей и представителей администрации. За время работы система контент-фильтрации показала себя надежной, эффективной и удобной в использовании.

В проекте «Безопасная информационно-образовательная среда как условие формирования культуры в информационном пространстве МБОУ «Воротынская СШ» (авторы: А. А. Сергеев, Т. Ю. Рыбаков, Н. В. Козина, Е. Ю. Подневич)

безопасность локальной сети школы обеспечивается с помощью программного продукта компании «А-Реал Консалтинг» — «Интернет Контроль Сервер» (ИКС). ИКС полностью отвечает требованиям законов РФ № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию» и № 149 «Об информации, информационных технологиях и о защите информации».

Все компьютеры образовательной организации, используемые в учебном процессе, объединены в единую локальную сеть по проводной и беспроводным линиям. Для всех компьютеров локальной сети разрешен доступ к сети Интернет. Каждому компьютеру и пользователю назначен ряд правил и ограничений для доступа к тем или иным ресурсам интернета. В школе создана единая база цифровых образовательных ресурсов, доступ к которой разрешен всем пользователям локальной сети.

Схема локальной сети — классическая. В ее основе лежит сервер, через который происходит выход в интернет. В двух зданиях школы находятся коммутаторы, подключенные к серверу. От коммутаторов идет разводка на компьютеры учащихся и преподавателей. В сервере есть вся основная база ЦОР и установлено ПО для обеспечения безопасности локальной сети.

Архитектура информационно-коммуникационной системы многоуровневая. Межсетевой экран интеллектуально анализирует трафик и совместно с детектором атак предотвращает атаки хакеров, позволяет выявить подозрительную активность в локальной сети. Встроенный антивирус Dr.Web сканирует трафик на вирусы и блокирует вредоносное содержимое. Облачный сервис SkyDNS осуществляет блокировку нежелательных сайтов на уровне доменных имен.

Наборы правил блокируют сайты по встроенным категориям и имеют возможность добавления своих списков запрещенных сайтов. Специальные правила активируют безопасный поиск на сервисах Яндекс и Google. Ряд дополнительных правил, например блокировка торрент-трафика и ограничения скорости, позволяет полностью контролировать

сетевой трафик. Технология DLP предотвращает утечки конфиденциальной информации из внутренней сети, работает по ключевым словам и отпечаткам файлов. Встроенный модуль контент-фильтра блокирует страницы по спискам ключевых слов с сайтов Минюста, Роскомнадзора и сервиса SkyDNS.

В дополнение к защите ИКС на каждой рабочей станции установлено сертифицированное антивирусное решение от компании ESET. Все подключенные USB-накопители и компакт-диски проходят автоматическую проверку в фоновом режиме на наличие вредоносных программ. Встроенная в антивирус функция защиты доступа в интернет эффективно блокирует сайты с вредоносным содержимым.

Для доступа в интернет на компьютерах установлены актуальные версии браузеров Mozilla Firefox и Chromium с установленным расширением Adguard — интернет-фильтр для защиты пользователей от опасных веб-сайтов, блокировки всевозможных видов рекламы в интернете. Расширение представляет собой отличное дополнение к основной антивирусной защите с эффективной блокировкой вредоносных, мошеннических и фишинговых ресурсов, ускоряет загрузку страниц и экономит трафик.

Схема контентной фильтрации и защиты рабочего места Воротынской школы представлена на рисунке 9 (с. 48).

Средняя школа № 151 с углубленным изучением отдельных предметов Нижнего Новгорода представила проект «Создание безопасной среды школы» (автор Т. Г. Силантьева), в котором показано использование системы фильтрации веб-контента «ЭТИКУМ», разработанной ООО «Сетевые экспертные системы». Данная фильтрация полностью обеспечивает среду безопасного использования интернета, соответствующую требованиям ФЗ № 436.

Система контент-фильтрации обеспечивает возможность оперативной настройки компьютеров в зависимости от класса, расписания и многих других факторов. Она удобна в использовании и дает возможность информировать, разрешать или запрещать работу с различными ресурсами. Система

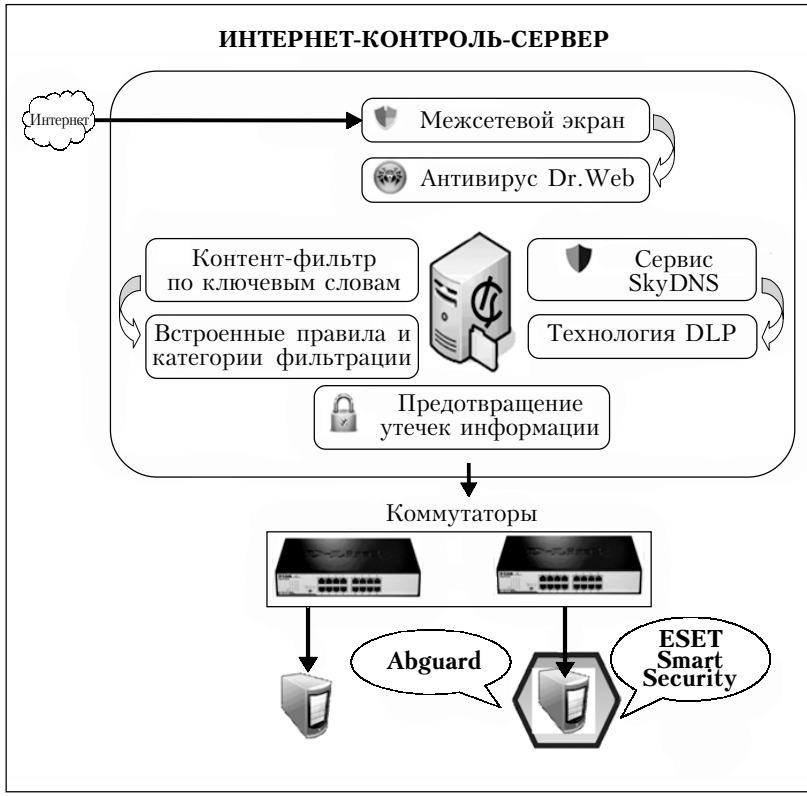


Рис. 9. Схема контентной фильтрации и защиты рабочего места МБОУ «Воротынская СШ»

учитывает также возрастное ограничение и список тематических категорий. Есть еще три удобные возможности, которые появились в процессе апробации:

- возрастная фильтрация по расписанию работы кабинетов информатики, при которой вводится расписание на всю четверть и по часам и системой включается нужный профиль;
- возможность централизованной дистанционной групповой и локальной настройки;
- мониторинг информации по выходу в интернет со всех школьных компьютеров.

На основе данной системы контент-фильтрации в школе планируется сделать удобную разновозрастную домашнюю контент-фильтрацию, которую можно будет предложить родителям для установки на домашних ПК учащихся.

В *номинации «Организационно-управленческое решение создания безопасной информационной образовательной среды образовательной организации»* победителями и призерами стали: МБОУ «Лицей № 3» Кулебак (1-е место), МБОУ «Гимназия» Арзамаса (2-е место), МБОУ «Школа № 173 с углубленным изучением отдельных предметов» Нижнего Новгорода (3-е место).

В данной номинации представлены: описание мероприятий; перечень законов и нормативных актов, на которые опирается образовательная организация в реализации единой политики в сфере защиты детей от информации, причиняющей вред их здоровью и развитию; локальные акты, правила, процедуры, обеспечивающие защиту личной информационной среды обучающегося на законодательной и правовой основе.

Победитель в номинации — МБОУ «Лицей № 3» Кулебак — представил проект «Межмуниципальный центр инновационного образования» (авторы: Е. Е. Кощеева, Т. Н. Лебедева, Е. В. Дегтярева). Концептуальная идея проекта заключается в создании открытой безопасной информационной образовательной среды, уникальной в своем развитии, но в то же время являющейся частью информационной системы муниципального, межмуниципального и регионального образований.

Успешное функционирование безопасной информационной образовательной среды межмуниципального центра инновационного образования основано на организации четкой работы десяти модулей информационно-образовательной среды: административного модуля, модуля методической службы, учебного модуля, модуля инновационной и научной работы, модуля медиацентра, модуля информационной службы, модуля дополнительного образования, модуля здоровьесберегающих технологий, модуля воспитательной системы,

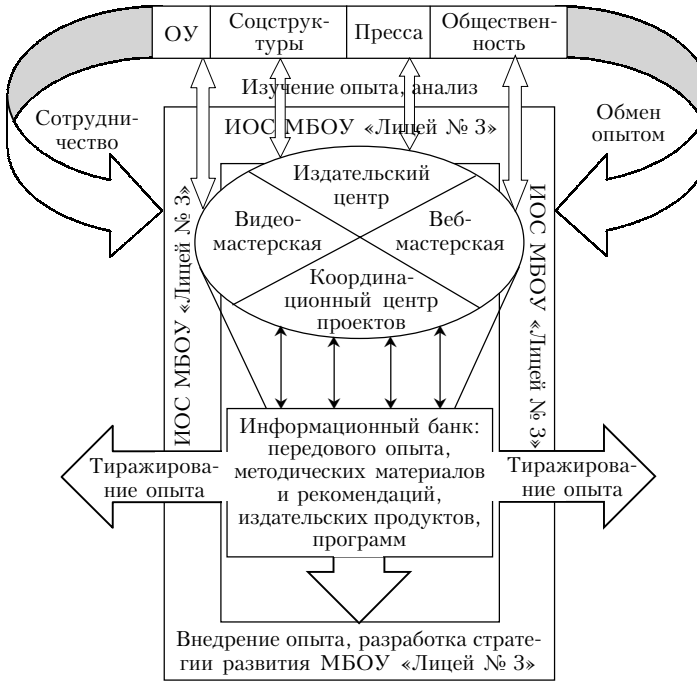


Рис. 10. Взаимодействие модулей информационно-образовательной среды лицея

модуля психолого-социального сопровождения. Взаимодействие модулей информационно-образовательной среды лицея представлено на рис. 10.

Связующим звеном эффективного функционирования всех модулей информационно-образовательной среды межмуниципального центра инновационного образования является модуль информационной службы, работа которого представлена четырьмя взаимосвязанными блоками.

- Издательский блок: пресс-центр «Фотон+» (5—11-е классы), пресс-центр «Светлячок» (1—4-е классы), информационный центр сообщества «Школьные СМИ Нижегородской области».
- Координационный блок: сопровождение региональной интернет-викторины «Наследие земли Нижегородской»,

«Сеть опорных площадок школиздата России», мероприятий Всероссийской интеллектуальной олимпиады для школьников «Наше наследие» на муниципальном и региональном уровнях.

➠ Творческий блок: «Веб-мастерская», «Видеомастерская».

➠ Информационный блок: сопровождение системы «Дневник.ру» в школе.

Представленная модель безопасной информационной образовательной среды лицея способствует не только повышению эффективности обучения и воспитания школьников, но и формированию культуры грамотного сетевого общения взрослого и ребенка через совместную практическую деятельность.

Основным ресурсом данной модели безопасной информационной образовательной среды является образовательный портал инновационных проектов, где созданы необходимые условия для эффективного сетевого партнерства образовательных организаций и личностно ориентированного развития взрослых и детей. Сотрудничество педагогов и школьников на муниципальном, межмуниципальном, региональном и всероссийском уровнях обеспечено действующими переговорными виртуальными площадками, совместными сетевыми ресурсами, системой мастерских и вебинаров.

Для педагогов и родителей на уровне межмуниципального образования реализуется система тьюторского сопровождения повышения ИКТ-компетентности, в том числе по вопросам организации безопасного использования образовательных ресурсов сети Интернет. Действует сетевая мастерская для родителей, представленная на портале особыми рубриками: «Рекомендации для родителей», «Советы специалиста», «СанПиНы об использовании ЭОР и технических устройств в учебном процессе», «Техническая поддержка обеспечения безопасности в сети Интернет».

Для школьников безопасное использование разнообразных информационных образовательных ресурсов обеспечено системой необходимых мероприятий (классных часов,

акций, онлайн-форумов) и рубрик портала: «Рекомендации для школьников», «Советы психолога», «Горячие телефоны по вопросам обеспечения безопасности в сети Интернет».

Проект моделирования безопасной информационной среды МБОУ «Гимназия» Арзамаса «РАДУNET» (авторы: И. А. Кузьмичева, С. В. Краснов) реализуется в образовательной организации с 2014 года и осуществляется через техническую, нормативную, учебно-методическую компоненты. Особое внимание в проекте уделяется учебно-методической компоненте, которая реализуется через следующие системообразующие модули:

- Модуль «Родитель — ученик» направлен на построение траектории сотрудничества и положительного взаимодействия детей и их родителей по проблеме проекта через участие в ежегодных общешкольных конкурсах, таких как семейный конкурс буклетов «Интернет и безопасность» (5—6-е классы), конкурс рисунков «Наш интернет!» (1—4-е классы).
- Модуль «Родитель — родитель» обеспечивает возможность конструктивного обсуждения родителями учащихся модели безопасной информационной среды гимназии через участие в общешкольной акции «Генератор идей. Навстречу безопасности!» (9—11-е классы).
- Модуль «Родитель — ученик — учитель» организует взаимосвязанную деятельность всех субъектов образовательного пространства гимназии, создает возможность обмена мнениями, координации деятельности по конструированию модели безопасной информационной среды гимназии. Примеры мероприятий — творческий литературный конкурс «Моя информационная среда», выпуск электронного вестника «Моделирование безопасной информационной среды МБОУ “Гимназия” Арзамаса».
- Модуль «Ученик — ученик» способствует развитию самостоятельности, универсальных учебных действий у школьников через организацию и планирование деятельности команды юниор-тьюторов «Наш РАДУNET!» (1—4-е классы).

В ходе реализации проекта разработаны несколько сцена-

риев в игровой форме для младших школьников, проведены десять занятий.

Реализация проекта «РАДУНЕТ» ориентируется на построение конструктивного взаимодействия между субъектами образовательного пространства школы.

МБОУ «Школа № 173 с углубленным изучением отдельных предметов» Нижнего Новгорода представила проект «Неделя безопасного интернета в начальной школе» (автор И. В. Соловьева). Предлагается программа проведения Недели безопасного интернета в начальной школе; разработаны мероприятия, привлекающие внимание к проблеме безопасности детей и взрослых в сети Интернет, в том числе классные часы, родительские собрания и семинары для педагогов; подготовлен объемный пакет дидактических материалов для использования в рамках мероприятий Недели.

Научно-методическое и дидактическое обеспечение безопасной информационной образовательной среды образовательной организации включает:

- мероприятия, направленные на формирование у подрастающего поколения, родителей и педагогов культуры безопасности, ответственности за осуществленные действия в информационном пространстве;
- мероприятия и документы, направленные на актуализацию потребности школьников в здоровом образе жизни, на снижение и профилактику компьютерной и интернет-зависимости среди учащихся;
- организацию нравственного и этического контроля.

Места в соответствующей *номинации — «Научно-методическое и дидактическое обеспечение безопасной информационной образовательной среды образовательной организации»* — распределились следующим образом: 1-е место — МБОУ «СШ № 14» Дзержинска, 2-е место — МБОУ «Арьёвская СШ» Уренского района, 3-е место — МБОУ «Школа № 7» Кулебак.

Целью проекта «Безопасная информационная образовательная среда МБОУ “Средняя школа № 14” (Дзержинск)» (автор Н. А. Рыганов) стали разработка и внедрение моде-

ли формирования безопасной информационной образовательной среды образовательной организации.

В проекте обозначены основные направления формирования безопасной информационной среды ОО:

- создание единого информационного пространства;
- обеспечение компьютерной поддержки учебной деятельности на основе новых информационных технологий;
- создание единой автоматизированной системы обеспечения учебной, образовательной, методической информацией;
- создание системы электронного документооборота;
- разработка системы мероприятий по формированию безопасной информационной среды ОО;
- разработка и внедрение мониторинга уровня сформированности информационной культуры участников образовательной деятельности и уровня безопасности информационной среды.

Особый интерес представляет информационный ресурс (сайт), обеспечивающий информационную и методическую поддержку педагогов школы. На сайте представлены разнообразные материалы: план реализации проекта, методические разработки, анкеты, опросники.

МБОУ «Арьёвская средняя общеобразовательная школа» Уренского района представила проект «Неделя безопасного интернета» (автор И. Б. Баранцева), основной идеей которого стала разработанная система мероприятий по информированию родителей и учащихся о рисках в сети Интернет. Для этого школа проводит ежегодную Неделю безопасного интернета, основой которой является кейсовая технология. Изучая содержимое кейса, учащиеся повторяют правила безопасной работы в интернете, знакомятся с новой интересной технологией представления информации (скрайбинг, фотокомиксы), выполняют творческое задание, размещают его в безопасной среде, обмениваются мнениями по выполнению работ с другими участниками (Приложение 10).

Проект «Интернет — вместе к территории безопасности» разработан творческой группой педагогов МБОУ «Школа № 7» Кулебак (авторы: В. Е. Зуева, Л. Н. Игошина, Е. Г. Кошелева, Т. О. Кузнецова, С. В. Ладыгина, Т. Ю. Лялина, Н. К. Морозова, М. Н. Морозова, Е. П. Соколова, Т. В. Хохлова). Для консолидации усилий обучающихся, родителей, педагогов в работе, направленной на сведение к минимуму негативного влияния интернета, в образовательной организации создано объединение «Кибердружина». Актив «Кибердружины» составили учащиеся 8—10-х классов, представители ОПДН, а также УУП и ПДН Отдела МВД России по Кулебакскому району. В плане работы объединения — проведение акций, лекториев, внеклассных мероприятий для учеников; организация совместных с родителями и социальным психологом школы рейдов «Родительский патруль». На сайте образовательной организации создана тематическая страница, содержащая материалы проекта и информацию для широкого круга лиц по теме «Интернет-безопасность».

Партнером проекта — газетой «Земля Нижегородская» (главный редактор Е. Ю. Беляева) в числе представленных на конкурс работ отмечен проект МБОУ «Вязовская ОШ» Тонкинского района. Замысел и реализация проекта представляли собой инициативную деятельность учащихся под руководством педагога (С. В. Баева, учитель информатики).

Методом «мозгового штурма» ребята поставили цель и задачи, разработали этапы реализации и их содержание, определили материальные и технические ресурсы, распределили обязанности каждого. В ходе основного этапа проекта учащиеся работали фронтально с информационными ресурсами, в том числе с информацией, размещенной на сайтах производителей антивирусных программ, таких как Лаборатория Касперского и Доктор Вэб, на сайте «Microsoft. Центр безопасности»; выясняли вопросы безопасности информационных систем с системным администратором района.

Результатами проекта стали социальный видеоролик «Безопасный интернет», в котором были собраны основные пра-

вила безопасной работы в интернете, буклет «Правила безопасного интернета», сценарий и проведение общешкольного мероприятия «Безопасность в интернете».

Творческие конкурсы как средство стимулирования творческой активности учащихся и педагогов

Важным фактором, способствующим привлечению внимания к вопросам БИОС, являются творческие конкурсы и проекты. Так, ПАО «Ростелеком», один из крупнейших российских провайдеров, помимо основного направления по предоставлению услуг связи и телекоммуникационных сервисов ведет работу с различными целевыми аудиториями. Например, для пожилых людей компания создала сайты (http://азбукаинтернета.рф/ и http://azbukainterneta.ru/) и выпустила учебное пособие «Азбука Интернета», благодаря которым пенсионеры могут получать знания о возможностях персонального компьютера, научиться пользоваться интернетом, электронной почтой, социальными сетями. Кроме того, каждый год для людей пожилого возраста проводится конкурс «Спасибо Интернету», показывающий личные достижения участников в изучении основ компьютерной грамотности.

Для представителей медиаиндустрии компания ежегодно организует международный конкурс журналистов и блогеров «Вместе в цифровое будущее» (http://smi.rt.ru). А для жителей Приволжского федерального округа, неравнодушных к своему краю, дважды проводился творческий конкурс «Я тут был», по итогам которого фоторепортажи и эссе участников и победителей вошли в две иллюстрированные книги «Неизведанное Поволжье» и «Неизведанное Поволжье 2.0» (http://www.events.volga. rt.ru/?id=5861).

Не оставлены в стороне детская и подростковая аудитории. На протяжении трех лет на территории Поволжья проводился конкурс детских творческих работ «Безопасный

Рис. 11. Постер конкурса «Безопасный Интернет»

Интернет» (см. рисунок 11). Конкурс был организован с целью формирования у детей и молодежи навыков безопасного и ответственного поведения в сети Интернет, а также получения ими знаний о социальных последствиях неправильного поведения во Всемирной паутине. Компания также привлекала внимание общественности к вопросам информирования детей и родителей об угрозах и рисках при работе с открытыми источниками в интернете, адекватного отношения к получаемому из сети контенту и защите персональных данных.

Ежегодный конкурс стартовал осенью накануне учебного года и длился до февраля следующего года. В осенне-зимний период актуальная тематика конкурса имела все шансы привлечь внимание большого числа детей и подростков. Проводилась активная кампания по продвижению конкурса в социальных сетях, на ведущих информационных порталах регионов, на школьных сайтах и других тематических площадках; в жюри привлекались представители региональ-

ных министерств связи, ведущие педагоги, уполномоченные по правам ребенка в ПФО, общественные деятели, представители СМИ. Итоги конкурса были подведены накануне Международного Дня безопасного Интернета в феврале.

К участию в конкурсе приглашались учащиеся общеобразовательных организаций, а также студенты 1—2-х курсов организаций начального и среднего профессионального образования ПФО (за исключением Пермского края) в возрасте от 7 до 17 лет. Предоставить свои работы на конкурс могли отдельные ученики, группы учеников или творческие группы и целые классы.

Для объективной оценки участники были разделены на три возрастные категории: с 7 до 10 лет, с 11 до 13 лет, с 14 до 17 лет. Возрастная категория в случае участия в конкурсе детей разного возраста определялась по возрасту старшего участника.

В оригинальной и художественной форме отразить тему безопасного Интернета предлагалось по трем номинациям:

- «Видеоролик» (для всех возрастных категорий);
- «Рисунок» (для возрастной категории 7—10 лет) / «Социальный плакат» (для возрастных категорий 11—13 лет и 14—17 лет);
- «Стихотворение» (для всех возрастных категорий).

Жюри при оценке конкурсных работ обращало внимание на оригинальность творческой задумки, мастерство и качество исполнения, соответствие работы заданной тематике, использование различных методов исполнения. Темы творческих работ: вредоносные программы и спам, мошенничество и пиратство в интернете, опасный контент в сети, ответственное поведение в социальных сетях.

Работы участников конкурса оценивались вначале на региональном уровне, где определялись победители в каждой из трех возрастных категорий в каждой номинации. Второй этап — межрегиональный, на котором жюри выбирало лучшие работы из победителей в 13 регионах ПФО. Все участники награждались дипломами «Ростелекома», а победители получили ценные призы — электронные девайсы, моде-

ли с дистанционным управлением, игровые приставки, сертификаты на покупку товаров для учебы и отдыха.

Техническое и организационное сопровождение конкурса осуществлялось силами сотрудников департамента внешних коммуникаций макрорегионального филиала «Волга» ПАО «Ростелеком». Для проведения конкурса использовался собственный ресурс компании http://www.events.volga.rt.ru с личным кабинетом для участников и жюри. Также на ресурсе были размещены все необходимые для участия в конкурсе материалы: правила участия, материалы для родителей и детей (тест для родителей, советы психолога, полезные ссылки для учебы и отдыха).

Рис. 12. Плакат для продвижения конкурса

Для привлечения внимания к конкурсу и возможной профилактики безопасного использования сети Интернет среди детской аудитории в партнеры третьего конкурса был приглашен Координационный совет уполномоченных по правам ребенка в ПФО. Этапы проведения конкурса и его результаты освещались в региональных СМИ, также были выпущены видеоновости для соцсетей по итогам трех конкурсов. Плакат для продвижения конкурса представлен на рисунке 12.

Год от года конкурс менялся и привлекал все больше детей и подростков. Помимо школьников, к участию были привлечены учащиеся техникумов и ПТУ, интерес детей и подростков повышался с введением новых номинаций, появились новые партнеры. Сравнительная характеристика трех конкурсов приведена в таблице на с. 60—61.

Развитие конкурса по периодам проведения

Показатели	Периоды проведения		
	2012—2013 гг.	**2013—2014 гг.**	**2014—2015 гг.**
Номинации	Видеоролики	Видеоролики	Видеоролики Стихотворения Рисунки / плакаты
Учебные заведения	Ученики школ в возрасте 8—17 лет	Ученики школ в возрасте 8—17 лет Учащиеся 1—2-х курсов организаций начального и среднего профессионального образования	Ученики школ в возрасте 7—17 лет Учащиеся 1—2-х курсов организаций начального и среднего профессионального образования
Количество работ	406	300	2350 Видеоролики — 11 % Стихотворения — 22 % Рисунки / плакаты — 67 %
Регионы ПФО	13 регионов Более 70 % работ — из населенных пунктов по статусу ниже районного центра	12 регионов Более 60 % работ — из отдаленных от региональных столиц населенных пунктов	13 регионов Более 50 % работ из районных центров, сел и деревень
Интересные факты	Суммарное время присланных видеороликов превышает 14 часов. За время проведения конкурса официальный сайт по-	Суммарное время присланных видеороликов превышает 10 часов. За время проведения конкурса официальный сайт посетили более 40 тыс. человек. Самое	Самыми активными участниками конкурса стали учащиеся в возрасте от 14 до 17 лет. Самое большое количество работ — из Республики Татарстан

Окончание табл.

Показатели	Периоды проведения		
	2012—2013 гг.	**2013—2014 гг.**	**2014—2015 гг.**
	сетили более 6 тыс. человек. Самое большое количество работ — из Республики Татарстан	большое количество работ — из Нижегородской области	
Партнеры	—	—	Координационный совет уполномоченных по правам ребенка ПФО

Проект реализован. Что дальше? Конкурс, проводимый «Ростелекомом» в ПФО, получил развитие на федеральном уровне. Компания организовала новый конкурс — «Классный Интернет», целями которого являются выявление лучших школьных проектов в области интернет-технологий, повышение престижа работы педагогов в этой сфере (www.safe-internet.ru). Побороться за звание лучшего можно не только единолично, но и в составе целой команды, отправив свои проекты по нескольким номинациям.

В настоящее время материалы конкурса широко используются «Ростелекомом» в волонтерской деятельности для проведения уроков по безопасной работе в сети Интернет, родительских собраний, внешних молодежных мероприятий и акций. Работы победителей планируется размещать в качестве пропаганды безопасного интернета в социальных сетях и блогосфере. ☺

Литература

1. *Абрамова, С. В.* Реализация системного подхода в построении методической системы подготовки специалистов в образовательной области безопасности жизнедеятельности / С. В. Абрамова, Е. Н. Бояров // В мире научных открытий. — 2011. — № 4.1. — С. 397—404.

2. *Авдеева, Н. В.* Роль культуры в системе подготовки бакалавров образования в области безопасности жизнедеятельности / Н. В. Авдеева, Е. А. Бырылова, П. В. Станкевич // Мир науки, культуры, образования. — 2012. — № 5. — С. 36—39.

3. *Алисов, Е. А.* Разработка и обоснование концепции формирования экологически безопасной образовательной среды / Е. А. Алисов // Ученые записки : Электронный научный журнал Курского государственного университета. — 2011. — № 17. — С. 182—187.

4. *Бармин, Н. Ю.* Информатизация нижегородской школы: состояние и перспективы / Н. Ю. Бармин // Нижегородское образование. — 2009. — № 2. — С. 23—30.

5. *Бояров, Е. Н.* Безопасная информационная образовательная среда вуза: понятие и компоненты / Е. Н. Бояров // Молодой ученый. — 2014. — № 18.1. — С. 20—23.

6. *Бояров, Е. Н.* Экология информационной образовательной среды / Е. Н. Бояров // Астраханский вестник экологического образования. — 2012. — № 3. — С. 78—84.

7. *Вылегжанина, И. В.* Безопасность ребенка в информационном обществе : методические рекомендации для образовательных учреждений по проведению родительского всеобуча на тему детской безопасности в Интернете / И. В. Вылегжанина. — Киров : КОГ АУ ДПО (ПК) «ИРО Кировской области», 2011. — 17 с.

8. *Гладышева, О. С.* Дистанционное повышение квалификации педагогов по актуальным вопросам здоровьесберегающей деятельности в образовательной организации / О. С. Гладышева, И. Ю. Абросимова, Е. Е. Кузоватова // Нижегородское образование. — 2017. — № 1. — С. 79—85.

9. *Ерофеева, А. О.* Методические рекомендации по обеспечению информационной безопасности обучающихся системы профессионального образования [Электронный ресурс] / А. О. Ерофеева [и др.]. — Режим доступа: http://ptu53.ucoz.ru/metodicheskie_rekomendacii_po_obespecheniju_ inform.pdf.

10. Интернет: возможности, компетенции, безопасность : методическое пособие для работников системы общего образования [Электронный ресурс]. — Режим доступа: http://goo.gl/FXhGiP.

11. *Калинкина, Е. Г.* Формирование информационного общества и развитие ИКТ-компетентности педагогов в процессе повышения квалификации / Е. Г. Калинкина // Нижегородское образование. — 2009. — № 4. — С. 4—11.

12. *Канянина, Т. И.* Этические и правовые нормы информационной деятельности человека / Т. И. Канянина, Н. О. Кудин // Мир компьютерных технологий : сборник статей по материалам Региональной студенческой научно-практической конференции. — Н. Новгород : Нижегородский государственный педагогический университет им. К. Минина, 2016. — С. 3—5.

13. Лаборатория Касперского. Об угрозах [Электронный ресурс]. — Режим доступа: http://www.kaspersky.ru/internet-security-center.

14. Майкрософт. Центр безопасности [Электронный ресурс]. — Режим доступа: https://www.microsoft.com/ru-ru/security/.

15. Методика организации недели «Безопасность Интернет» : методические рекомендации / авт-сост. : О. В. Селиванова, И. Ю. Иванова, Е. А. Примакова, И. В. Кривопалова. — Тамбов : ИПКРО, 2012 ; http://spuzt1.ru/InfBezop/anketa_ostorozhno_virus.pdf.

16. *Пичененко, В. Г.* Основы безопасности жизнедеятельности : методическое пособие / В. Г. Пичененко, Е. Е. Конюхов, И. Ю. Молев, П. В. Игнатьев, И. И. Бондарева. — Н. Новгород : Нижегородский институт развития образования, 2010. — 195 с.

17. Постановление Правительства Российской Федерации от 23 мая 2015 г. № 497 «О Федеральной целевой программе развития образования на 2016—2020 годы».

18. Приказ Минтруда России от 18.10.2013 № 544н «Об утверждении профессионального стандарта “Педагог (педагоги-

ческая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)"» [Электронный ресурс]. — Режим доступа: http://www.rosmintrud.ru/docs/mintrud/orders/129/.

19. Проект концепции и содержания профессионального стандарта учителя [Электронный ресурс]. — Режим доступа: http://минобрнауки.рф.

20. *Рубцова, О. В.* Экспертиза информационной безопасности образовательной среды / О. В. Рубцова, Е. В. Якушкина // Педагогическая диагностика. — 2014. — № 5. — С. 3—12.

21. *Силюк, А. М.* Информационная безопасность детей и подростков в сети Интернет [Электронный ресурс] / А. М. Силюк. — Режим доступа: http://spuzt1.ru/InfBezop/klassnyj_chas_internet.pdf.

22. Социальный видеоролик «Безопасный Интернет» [Электронный ресурс]. — Режим доступа: https://yadi.sk/i/_M8hcJSMqdXL4.

23. ФГОС ООО: Федеральный государственный образовательный стандарт основного общего образования. — М. : Просвещение, 2011. — 61 с.

24. Федеральные государственные образовательные стандарты общего образования [Электронный ресурс]. — Режим доступа: минобрнауки.рф/документы/543.

25. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ.

26. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г. У. Солдатова, Т. А. Нестик, Е. И. Рассказова, Е. Ю. Зотова. — М. : Фонд Развития Интернет, 2013. — 144 с.

Материалы, представленные участниками конкурса «Безопасная информационная образовательная среда образовательной организации»

Приложение 1

Годовой план мероприятий по теме «Безопасный интернет»

МБОУ «Школа № 105» Н. Новгорода

№ п/п	Наименование мероприятия	Сроки	Ответственные
1	Изучение нормативных документов по организации безопасного доступа к сети Интернет. Формирование нормативно-правовой базы	Январь — август	Заместитель директора по информатизации
2	Разработка уроков безопасности работы в интернете для учащихся 1—4, 5—9, 10—11-х классов	В течение учебного года	Классные руководители 1—11-х классов
3	Организация и проведение конкурса детских работ «Мой безопасный интернет»	Февраль	Заместитель директора по воспитательной работе

Продолжение табл.

№ п/п	Наименование мероприятия	Сроки	Ответственные
5	Тематические уроки информатики (5—11-е классы)	В течение учебного года	Учителя информатики
6	Выступление педагога-психолога на общешкольном родительском собрании на тему «Интернет в жизни вашего ребенка»	В течение учебного года	Педагог-психолог
	Индивидуальная работа педагога-психолога с обучающимися (по запросу родителей)	В течение учебного года	
	Правила для родителей «Как избежать интернет-зависимости ребенка»	Сентябрь	
7	Беседы с родителями на классных родительских собраниях по безопасному поведению детей в сети Интернет	В течение учебного года	Классные руководители
8	Организация работы группы «Юниор-тьютор "ЮнитиК"» с целью информирования обучающихся младших классов о безопасном поведении в сети Интернет Распространение памяток, листовок по правильному поведению в сети Интернет	В течение учебного года	Руководитель группы «Юниор-тьютор "ЮнитиК"»
9	Создание в локальной сети копилки методических разработок «Безопасный интернет» (разработки классных часов, родительских собраний, внеурочных мероприятий и т. д.)	В течение учебного года	Классные руководители
10	Оформление классных уголков по теме «Безопасный интернет»	В течение учебного года	Классные руководители

Окончание табл.

№ п/п	Наименование мероприятия	Сроки	Ответственные
11	Оформление школьных стендов по теме «Безопасный интернет»	В течение учебного года	Заместитель директора по воспитательной работе
12	Создание на сайте школы страницы «Безопасный интернет» и размещение информации по безопасному поведению в сети Интернет	В течение учебного года	Заместитель директора по информатизации
13	Создание каталога ссылок на тематические ресурсы в сети Интернет, обучающих правильному поведению в сети Интернет, и размещение его на сайте школы	В течение учебного года	Заместитель директора по информатизации
14	Выпуск тематических номеров газеты «Стопятка»	В течение учебного года	Руководитель газеты «Стопятка»
15	Участие обучающихся в конкурсах по безопасному интернету	В течение учебного года	Классные руководители, учителя-предметники

Приложение 2

План работы педагога-психолога по реализации программы первичной профилактики компьютерной и игровой зависимости среди несовершеннолетних

МБОУ «Школа № 105» Н. Новгорода

Система первичной профилактики компьютерной и игровой зависимости имеет свои этапы, которые позволяют не только взять ситуацию под контроль, но и существенно снизить количество детей, находящихся в группе риска.

№ п/п	Сроки проведения	Содержание мероприятий
1-й блок	Сентябрь — октябрь	Психологическое исследование. Диагностика по выявлению наличия признаков компьютерной и игровой зависимости. Методики Леонгарда, Кулакова, Никитина, Такера
		Тематическое выступление на родительском собрании «Ребенок и компьютер. Опасная грань»
		Выступление «Причины возникновения аддиктивного поведения у несовершеннолетних» на педагогическом совете школы
		Тематический классный час для учащихся «Компьютер: за и против»
		Организация индивидуального консультирования детей, попавших в группу риска по результатам обследования
2-й блок	Ноябрь — декабрь	Беседы с родителями на темы: «Влияние компьютера на здоровье ребенка», «Значение игры в жизни ребенка»
		Упражнение для учащихся с элементами тренинга «Живое общение. Давайте наблюдать. Хорошо ли я знаю одноклассников?»
3-й блок	Январь — февраль	Беседы с родителями на тему «Появление и развитие одиночества у детей»
		Беседа с учащимися на тему «Позитивная виртуальность и девиртуализация»
4-й блок	Март — апрель	Повторная диагностика и анализ мониторинга полученных данных (методики Такера, Никитина, Кулакова)
		Конкурс плакатов, рисунков, слоганов учащихся «Жизнь в реале»
		Упражнение для учащихся и родителей с элементами тренинга «Связующая нить»

Приложение 3

Пример теста на тему «Безопасный интернет»

МБОУ «Школа №105» Н. Новгорода

№ 1 (*1 балл*)

Для того чтобы антивирусные программы обеспечивали наилучшую безопасность вашего ПК, необходимо:

☐ Установить несколько антивирусных программ

☑ Своевременно обновлять антивирусные базы

☐ Удалить все файлы, загруженные из сети Интернет

☐ Отключить компьютер от сети Интернет

№ 2 (*1 балл*)

Что необходимо сделать, если на сайте в Интернете вдруг появилось сообщение о быстрой проверке ПК с просьбой перезагрузки компьютера?

☐ Отформатировать жесткий диск

☐ Выключить компьютер

☐ Перезагрузить компьютер

☑ Закрыть сайт и выполнить проверку ПК

№ 3 (*1 балл*)

Спам — это:

☐ Компьютерный вирус, записывающийся в первый сектор гибкого или жесткого диска и действующий при загрузке компьютера

☐ Разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети

☑ Массовая рассылка коммерческой и иной рекламы или подобных коммерческих видов сообщений лицам, не выражавшим желания их получать

☐ Первый вирус, получивший значительное внимание со стороны средств массовой информации

№ 4 (*1 балл*)

Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям:

☐ Спам
☐ Троянская программа
☑ Фишинг

№ 5 (*1 балл*)

Специализированная программа для обнаружения компьютерных вирусов:

☐ Хакерские атаки
☑ Антивирус
☐ Фишинг

№ 6 (*1 балл*)

Что необходимо сделать, если на экране появилось окно с просьбой отправить SMS для дальнейшей работы?

☐ Отправить SMS-сообщение
☐ Выполнить форматирование жесткого диска
☐ Перезагрузить компьютер
☑ Не отправлять SMS-сообщение

№ 7 (*1 балл*)

Какие антивирусные программы вы знаете?

Ответ: Avast, Dr. Web, NOD32, Kaspersky (без учета регистра)

№ 8 (*2 балла*)

Как защитить себя от того, чтобы тебя не исключили из чата (беседы)?

☑ Соблюдать этикет общения
☐ Отвечать на сообщения только знакомым людям
☑ Не использовать фразы, запрещенные цензурой
☐ Отвечать всем собеседникам чата

№ 9 (*2 балла*)

Как защитить себя от баннера, блокирующего компьютер (веб-страницы)?

☐ Не совершать онлайн-покупок
☑ Не переходить по сомнительным ссылкам
☑ Пользоваться антивирусами, предоставляющими безопасный режим
☐ Пользоваться только одним браузером

№ 10 (*2 балла*)

Как защитить свой профиль от взлома?

☑ Никому не сообщать логин и пароль
☑ Установить надежный пароль
☐ В различных аккаунтах использовать одни и те же логин и пароль
☐ Не закрывать свой профиль на чужом компьютере

№ 11 (*1 балл*)

Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно…

☐ Административному кодексу
☐ Гражданскому кодексу
☑ Уголовному кодексу
☐ Трудовому кодексу

№ 12 (*2 балла*)

По каким признакам можно понять, что компьютер заражен вирусом?

☐ Компьютер работает в нормальном режиме
☑ Пропали файлы
☐ Подключение к Интернету отсутствует
☑ Программы не запускаются

№ 13 (*1 балл*)

Для чего делают резервные копии?

☐ Чтобы не потерять информацию
☐ Чтобы открыть текстовый документ
☑ Чтобы восстановить систему
☐ Чтобы информация была доступна всем в Интернете

№ 14 (*2 балла*)

Какой из браузеров считается менее безопасным, чем остальные?

☑ Internet Explorer
☑ Opera
☐ Google Chrome
☐ Mozilla Firefox

№ 15 (*1 балл*)

Сайт вдруг просит повторно ввести ваши логин и пароль, чего раньше никогда не было. Что вы сделаете?

☐ Введу данные, так как мой аккаунт привязан к телефону, значит, защищен

☑ Проверю адрес сайта; если он не совпадает с настоящим, закрою сайт

☐ Введу, раз нужно

Приложение 4

Методическая разработка классного часа по теме «Я выбираю безопасный интернет»

МБОУ «Школа №105» Н. Новгорода

Класс: 5-й.

Форма: игра.

Цель: актуализация потребностей соблюдения правил безопасной работы в сети Интернет.

Учебные задачи, направленные на достижение личностных результатов обучения:

- формирование коммуникативной компетентности в общении и сотрудничестве со сверстниками в исследовательской и творческой деятельности;
- развитие мотивов учебной деятельности и формирование личностного смысла учения;
- развитие самостоятельности и личной ответственности за свои поступки, принятые решения, выполненный творческий продукт.

Учебные задачи, направленные на достижение метапредметных результатов обучения:

- развитие умения работать с информацией (сбор, систематизация, хранение, использование);
- формирование умений целеполагания; планировать пути достижения целей; выделять альтернативные способы достижения цели и выбирать наиболее эффективный способ;
- формирование умений строить логическое рассуждение, включая установление причинно-следственных связей, делать умозаключения и выводы на основе аргументации;
- формирование умений организовывать и планировать учебное сотрудничество и совместную деятельность со сверстниками, самостоятельно и аргументированно оценивать свои действия и действия одноклассников;

➠ освоение умения планировать, координировать, контролировать и оценивать свою деятельность;

➠ развитие умения грамотно строить речевые высказывания в соответствии с задачами коммуникации;

➠ развитие умения слушать и слышать собеседника, вести диалог, излагать свою точку зрения, аргументировать ее;

➠ формирование умения взаимодействовать в статичных и мигрирующих группах в режиме интерактивного обучения, распределять роли и функции совместной проектной деятельности.

Учебная задача, направленная на достижение предметных результатов обучения: овладение основами безопасного пользования интернет-сетями.

Ключевой вопрос: Как организовать безопасную работу в сети Интернет?

Оборудование: мультимедийная презентация, карточки, картинки, кроссворды, ватман, маркеры, ручки, лист бумаги, листы взаимооценивания, клей-карандаш.

Предварительный этап

➠ Классный час с презентацией на тему «Безопасный интернет».

➠ Создание команд и выбор ими названий.

➠ Выполнение домашнего задания (создание слайда для презентации) каждой командой по своей теме: «Контентные риски интернета», «Интернет-зависимость», «Коммуникативные риски интернета», «Технические риски интернета», «Потребительские риски интернета».

Основной этап

1. Вводная беседа. Презентация «Безопасный интернет» (3—4 слайда).

2. Обсуждение цели игры: правила поведения в интернете и опасности интернета.

3. *Первый конкурс — МЫ СОСТАВЛЯЕМ.*

Пазл-картинка.

— Соберите картинку и поясните, что она выражает (часть картинок — за использование интернета, часть — против).

Дети собирают картинки и выражают свое мнение.

Выставление баллов.

4. *Второй конкурс — МЫ СОЧИНЯЕМ.*

— Составьте слоганы по теме безопасного интернета, используя слова «я», «моя семья», «мои друзья», «безопасность», «компьютер», «жизнь», «учеба», «игра», «плохо», «хорошо» (3—4 человека из команды).

Кто больше придумает слоганов?

5. *Третий конкурс — МЫ ПРЕЗЕНТУЕМ.*

Создание онлайн-презентации «Я за безопасный интернет».

Каждая команда выполняет дома задание по теме безопасного интернета. Результат своей деятельности ребята выносят на слайд в онлайн-презентации.

Защита своего слайда. Взаимооценивание команд по критериям.

Объявление предварительных результатов игры.

Критерии	**Баллы**	**Команды**			
		1	**2**	**3**	**4**
Содержание	От 5 до 2				
Дизайн	От 5 до 2				
Грамотность	От 5 до 2				
Представление	От 5 до 2				

Подведение итогов 2-го и 3-го конкурсов.

6. *Четвертый конкурс — МЫ СООТНОСИМ.*

— Соотнесите слово и его значение по типу «разрезной азбуки».

Время выполнения — 5 минут.

1. Банкинг *О*	Общее название технологий *дистанционного банковского обслуживания*
2. Блог *Т*	Веб-*сайт*, основное содержимое которого — регулярно добавляемые записи, содержащие текст, изображения или мультимедиа

Продолжение табл.

3. Виртуальный мир *B*	«Цифровые миры», «искусственные миры»
4. Вирус *E*	Вид *вредоносного программного обеспечения*, способность создавать копии самого себя и внедряться в код других программ, системные области памяти
5. Гейминг *T*	Форма *психологической зависимости*, проявляющаяся в навязчивом увлечении *видеоиграми* и *компьютерными играми*
6. Груминг *C*	Общение между взрослыми и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка
7. Кибербуллинг *T*	Агрессивное, умышленное действие, совершаемое группой лиц или одним лицом с использованием электронных форм контакта
8. Онлайн *B*	Нахождение индивида в сети Интернет
9. Офлайн *E*	Отсутствие индивида в сети Интернет
10. Сайт *H*	Совокупность логически связанных между собой веб-страниц; также место расположения контента *сервера*
11. Спам *H*	Массовая *рассылка* коммерческой и иной *рекламы* или подобных коммерческих видов сообщений лицам, не выражавшим желания их получать
12. Троллинг *O*	Вид виртуальной коммуникации с нарушением этики сетевого взаимодействия, выражающийся в виде проявления различных форм провокативного, агрессивного, издевательского и оскорбительного поведения
13. Фишинг *C*	Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям

Окончание табл.

14. Форум *Т*	Сайт (или соответствующее программное обеспечение) для интернет-общения
15. Чат *Ь*	Средство обмена сообщениями по компьютерной сети в режиме реального времени, а также *программное обеспечение*, позволяющее организовывать такое общение

Объяснение определений.

— Дополнительное задание: разложите все слова по алфавиту и получите еще одно слово. Объясните значение этого слова с точки зрения интернета.

Подсчет баллов. Подведение промежуточного результата.

7. *Пятый конкурс — МЫ РАССУЖДАЕМ.*

«Кто лишний?». По кругу расставляются стулья. Участников выбирается на одного больше, чем стульев. Ребята начинают двигаться вокруг стульев под музыку. Музыка заканчивается, участники садятся. Кто остался без стула, тот выходит из игры и забирает стул. На сиденье стула с обратной стороны есть предложение с многоточием. Прочитав его, участник должен вместо многоточия вставить слово «Родители» или «Дети».

1) … при общении в интернете нужно быть дружелюбными.

2) … чаще подвергаются буллингу в интернете.

3) … должны научиться спокойно правильно реагировать на обидные слова или действия других пользователей.

4) … могут заблокировать обидчика, написать жалобу модератору, потребовать удаления страницы.

5) … должны знать, с кем общаются … в сети.

6) … должны уметь не разглашать в интернете информацию личного характера.

7) … должны уметь не пересылать виртуальным знакомым свои фотографии или видео.

8) … должны разъяснить опасность встречи с незнакомыми людьми из интернета.

9) … на реальную встречу с интернет-другом обязательно должны ходить в сопровождении ….

10) …, объясните …, что в интернете тема любви часто представляется в неправильной, вульгарной форме.

11) … должны использовать технические средства ограничения доступа в интернет: родительский контроль, настройки безопасного поиска.

12) … должны рассказать … о негативной информации в сети.

13) … должны проверять сайты, которые посещают ….

14) … должны совершать покупки в интернете вместе с ….

15) …, не разрешайте … оплачивать покупки в интернете банковскими картами.

16) … никогда нельзя отправлять смс на короткие номера и оставлять на сомнительных сайтах номер телефона.

17) …, обсудите с … принципы мошенничества, проговорите правила безопасности и способы защиты.

18) … должны установить режим пользования интернетом для ….

19) …, попросите … в течение недели подробно записывать, на что тратится время, проводимое в интернете.

20) …, предложите … заняться чем-то вместе, постарайтесь увлечь, отвлечь от интернета.

Подсчет баллов за правильные ответы. Предварительный результат.

8. *Шестой конкурс — МЫ РЕШАЕМ.*

Кроссворд (см. с. 78). Время выполнения — 5 минут.

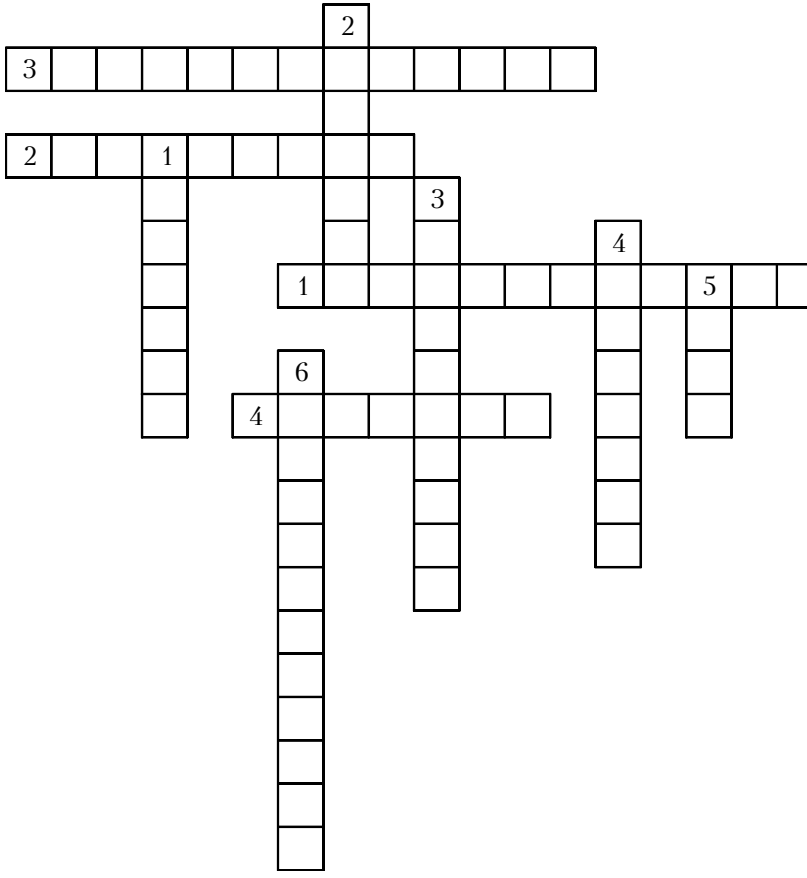
По горизонтали:

1) состояние защищенности;

2) устройство или система, способные выполнять заданную, четко определенную, изменяемую последовательность операций;

3) сложное слово (из двух корней), один из корней которого содержится в известной фразе героя мультфильма — кота Леопольда;

4) наполнение или содержание какого-либо сайта — текст, графика, музыка, видео, звуки и т. д.



По вертикали:

1) этим словом сегодня называют личную страницу интернет-пользователя на каком-либо сервисе;

2) сложный процесс взаимодействия между людьми, заключающийся в обмене информацией, а также в восприятии и понимании партнерами друг друга;

3) группа людей, имеющих общие интересы;

4) всемирная система объединенных компьютерных сетей для хранения и передачи информации;

5) совокупность компьютеров и различных устройств, обеспечивающих информационный обмен без использования

каких-либо промежуточных носителей информации (гибких дисков, компакт-дисков, флеш-карт и т. п.);

6) человек, который посещает интернет-пространство и пользуется действующей системой для того, чтобы выполнять конкретные задачи.

Подсчет баллов за правильные ответы. Предварительный результат.

9. *Седьмой конкурс — МЫ РИСУЕМ.*

Нарисуйте всей командой за одну минуту на ватмане, используя все маркеры, по количеству человек в команде, части компьютера — монитор, системный блок, принтер, колонки, мышь, клавиатуру.

Творческий конкурс оценивается одинаково для всех команд.

10. *Восьмой конкурс — МЫ ДУМАЕМ.*

Ребусы к словам. Каждая команда получает ребус, решает его и называет ответ, поясняя значение слова.

ТРОЛЛИНГ

КИБЕРБУЛЛИНГ

ГРУМИНГ




ГЕЙМИНГ




ФИШИНГ



Подсчет баллов за правильные ответы. Предварительный результат.

11. *Девятый конкурс — МЫ ЗНАЕМ.*

Правила безопасного интернета. Слова сложить в предложение (по типу «разрезной азбуки»). Наклеить готовые предложения на ватман.

1) Я при общении в интернете буду дружелюбным.

2) Я буду стараться быть спокойным в интернете.

3) Я должен научиться спокойно, правильно реагировать на обидные слова или действия других пользователей.

4) Я могу заблокировать обидчика, написать жалобу модератору, потребовать удаления страницы.

5) Я должен осторожно общаться в сети.

6) Я не должен разглашать в интернете информацию личного характера.

7) Я не должен пересылать виртуальным знакомым свои фотографии или видео.

8) Я должен знать опасность встречи с незнакомыми людьми из интернета.

9) Я не должен ходить на реальную встречу с интернет-другом.

10) Я должен знать, что в интернете тема любви часто представляется в неправильной форме.

11) Я понимаю, ограничение доступа в интернет — это моя безопасность.

12) Я должен рассказать взрослым о негативной информации в сети.

13) Я не должен доверять всем сайтам.

14) Я не должен совершать покупки в интернете.

15) Я не должен оплачивать покупки банковскими картами родителей.

16) Я никогда не буду отправлять смс на короткие номера и оставлять на сомнительных сайтах номер телефона.

17) Я должен знать принципы мошенничества и способы защиты в интернете.

18) Я должен быть в интернете не более 2 часов в день.

19) Я буду подробно записывать, на что тратится время, проводимое в интернете.

20) Я лучше займусь чем-то вместе с друзьями.

Подсчет баллов за правильные ответы.

Подведение итогов. Рефлексия игры.

Приложение 5

Методическая разработка родительского собрания по теме «Безопасность в интернете»

МБОУ «Школа №105» Н. Новгорода

Аудитория: родители учащихся 2-го класса.

Задачи:

➠ *образовательные*: формирование у родителей представления о роли, возможностях и способах использования

компьютера в обучении детей младшего школьного возраста;

➠ *воспитательные*: формирование у родителей представления о важности поддержания эмоционального контакта с ребенком во избежание развития у него компьютерной зависимости, для его безопасности в интернете;

➠ *организационные*: создание условий для привлечения родителей к организации экскурсий и работы компьютерного кружка;

➠ *информационные*: предоставление информации о психолого-педагогической и медицинской литературе, освещающей вопросы работы на компьютере младших школьников.

Подготовительный этап

1. Подбор и анализ литературы.
2. Совместная подготовка к собранию учителя, психолога, медицинского работника.
3. Составление перечня интересующих родителей вопросов.
4. Подготовка выставки развивающих компьютерных игр.
5. Подготовка проекта решения родительского собрания.

План родительского собрания

1. Вступительное слово учителя.
2. Вопросы к специалистам.
3. Проведение родительского собрания.
4. Подведение итогов.

Ход собрания

Вступительное слово учителя:

— Компьютеры уже давно проникли во все сферы нашей жизни. Они используются и на работе, и дома, и в школе, и даже в детском саду. С одной стороны, они облегчают нашу деятельность, а с другой — за удобства, скорость и комфорт мы вынуждены платить своим здоровьем. Так что же приносят компьютеры нашим детям — больше пользы или вреда? Как правильно организовать общение ребенка с компьютером? Сегодня мы ответим на эти вопросы.

Как правильно организовать рабочее место для ребенка за компьютером?

Для организации места для ребенка нужно установить удобную клавиатуру, найти мышь под его руку, удобный, регулируемый во всех плоскостях монитор. Особые требования предъявляются к освещенности помещения. Она не должна давать бликов на мониторе. Для этого нужно использовать дополнительное боковое освещение, лучше слева. Нельзя сидеть за компьютером в сумерках или темноте. Если что-то нужно перепечатывать с бумаги, то листы нужно установить как можно ближе к экрану для того, чтобы уменьшить разброс взгляда.

Памятка для родителей «Заболевания, которые могут возникнуть от неправильного использования компьютера»

Неправильная осанка	Последствия вредного излучения	Снижение зрения
Высота стула должна соответствовать длине голени, чтобы ступни всей поверхностью стояли на полу. Максимальная глубина сиденья должна составлять $^{2}/_{3}$ длины бедра, локти должны быть расположены как можно ближе к телу — угол между ними в плоскости тела не должен превышать прямого, во время работы с кла-	Мониторы компьютеров излучают в широких частотных диапазонах. Некоторая часть излучения приходится на инфракрасную, ультрафиолетовую и микроволновую части спектра, но в столь ничтожных интенсивностях, что этими составляющими можно пренебречь — они даже несоизмеримы с колебаниями естественного фона. Кроме того, мониторы порождают рентгеновское излучение, но оно практически полностью блокировано	После трех часов непрерывной работы за компьютером 88 % людей испытывают истощение системы зрения. При работе с монитором испытывается перенапряжение глазных мышц при длительной фокусировке на близких расстояниях. Для того чтобы восстановить энергетику и избежать истощения зрительной системы, следует отходить от компьютера не реже чем каждые полчаса. Работа за компьюте-

Окончание табл.

Неправильная осанка	Последствия вредного излучения	Снижение зрения
виатурой кисти рук должны быть максимально распрямлены	благодаря современным техническим решениям. Нужно сидеть от монитора на расстоянии вытянутой руки	ром формирует своего рода синдром «застывшего взгляда». Его нужно преодолевать сознательно и просто чаще моргать, тем самым снимая напряжение с мышц

Надо ли ограждать ребенка от компьютера (*выступление психолога*)

— Дети — группа риска, которые реагируют на все новое. С одной стороны, для развития детей компьютеры предоставляют благодатное поле. С другой — молодое поколение практически ничем не защищено. Дети даже не подозревают, как технологические новинки воздействуют на них. В случаях, когда тревожные симптомы действительно заметны, причем явно прослеживается их компьютерное происхождение, можно говорить о какой-то профилактике и ограничениях, но и в большинстве случаев лучший подход — относиться к указанным проблемам критично.

Способствует ли чрезмерное увлечение интернетом повышению агрессивности у ребенка?

Исследования А. Бандуры показали, что дети, в раннем возрасте предпочитавшие агрессивные телепередачи и фильмы, имели впоследствии конфликты с законом, иногда попадали в тюрьму. Даже если криминала не было, оставалось агрессивное отношение к своему окружению — детям, женам или мужьям, подчиненным. То есть то, что проявилось в 8—9-летнем возрасте, никуда не ушло, изменилась только форма. Выводы же относительно пагубного воздействия агрессивного телевидения в полной мере распространяются на компьютерные игры со сценами насилия. Степень совпадения с реальностью в последние годы достигла высокой отметки.

Опасные сайты в интернете

Депрессивные молодежные течения (депрессия — угнетенное, подавленное психическое состояние)

На сайтах обсуждаются способы причинения себе боли и вреда. Ребенок может поверить, что шрамы — лучшее украшение.

Сайты, на которых обсуждаются различные способы самоубийств и внушается мысль, что суицид — всего лишь способ избавления от проблем.

Сайты, на которых пропагандируется нездоровый образ жизни: анорексия (отказ от приема пищи) и булимия (чрезмерное употребление пищи), употребление алкоголя, табака и т. д.

Наркотики

Интернет пестрит новостями о «пользе» употребления марихуаны, рецептами и советами изготовления «зелья».

Сайты знакомств, социальные сети, блоги и чаты

Виртуальное общение разрушает способность к общению реальному (коммуникативный дисбаланс). Многие современные дети говорят, что у них нет или становится меньше друзей в школе, на улице, как это было раньше. В то же время в социальных сетях у ребят много знакомых, с которыми они готовы общаться.

Общаясь в сети, дети могут знакомиться и добавлять в друзья не известных им в реальной жизни лиц.

Злоумышленник, чаще всего представляясь сверстником, входит в доверие к ребенку, а затем пытается узнать личную информацию (адрес, телефон и др.) и договориться о встрече с целью совершения преступления, нередко прибегает к шантажу, эксплуатации. Ребенок может подвергнуться оскорблениям, запугиванию и домогательствам.

Кибербуллинг — запугивание, травля, физический и психологический террор, направленный на то, чтобы вызвать у жертвы страх и подчинить себе. Преследование, терроризирование осуществляется с помощью интернета и мобильного телефона (часто выкладывают ролики, в которых над кем-то издеваются, кого-то избивают).

Каждое слово, каждая выложенная в сети фотография могут быть использованы против человека.

Пропаганда азартных игр или агрессивных онлайн- (в реальном времени) *игр*

Нередко дети в поисках развлечений могут попасть на карточный сервер, на сайтах которого выложены игры на настоящие деньги (игровые сайты для детей содержат настольные и словесные игры с начислением очков, бывают условно-платные игры — приобретение различных опций).

Нецензурная брань, оскорбления

Экстремизм, национализм, фашизм

Информация, разжигающая расовую ненависть, нетерпимость по отношению к другим людям по национальным, социальным, групповым признакам.

Представители экстремистских течений используют все возможности интернета для того, чтобы заманить в свои ряды новичков.

Риск заражения ПК вредоносными программами (трояны, черви)

Вредоносные программы, кроме нанесения вреда хранящимся на компьютере данным, могут снижать скорость работы в сети и даже использовать компьютер для распространения вируса, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Потребительские риски

С ними встречаются люди, когда заказывают через интернет товары и услуги. Риск заключается в потере денежных средств без приобретения товара или приобретения товара низкого качества.

Хищение личной информации

Кража личных данных, или кибермошенничество, — когда происходит хищение личной информации, например паролей, имен пользователей, банковских данных, номеров кредитных карточек и т. д. Кража данных доступа к счету пользователей является наиболее распространенным видом мошенничества в интернете.

Интернет-зависимость

Это болезненное пристрастие, сильная психологическая привязанность к игре — в компьютерном варианте вплоть до желания жить в виртуальном мире. Тяжелые формы игровой зависимости предполагают крупные денежные траты на игру, злоупотребление кофе и энергетическими напитками, злость и раздражение при отрывании от игры, пренебрежение питанием и сном.

Зависимость от игр сравнима с наркотиками и алкоголем, человек не может контролировать свое времяпрепровождение за игрой, живет в собственном мире и не желает общаться с родными и друзьями.

Как же обеспечить безопасность работы детей в интернете?

Рекомендации для родителей

➠ Контролируйте деятельность детей в интернете с помощью современных программ. Установите и настройте средства фильтрации. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и что он на них делает.

➠ Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.

➠ Время, проводимое за компьютером, необходимо ограничить по причинам, связанным со здоровьем. Поместите компьютер в общей комнате. При использовании интернета младшими школьниками рекомендуется присутствие взрослого. Поощряйте детей среднего и старшего возраста делиться с вами опытом работы в интернете.

➠ Объясните ребенку, как важно использовать только проверенные информационные ресурсы и не использовать нелицензионные программы, в том числе скачанные из интернета.

➠ Периодически старайтесь полностью проверять свои рабочие компьютеры.

➠ Делайте резервную копию важных данных на внешнем устройстве — флеш-карте, диске.

➠ Старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли. То есть пароль должен быть не меньше 6 знаков, с использованием как букв, в том числе заглавных, так и цифр.

➠ Для того чтобы избежать отрицательных последствий при общении в интернете, следует придерживаться определенных правил, которым нужно научить детей:

— не нужно слепо верить в то, что собеседник говорит о себе;

— необходимо следить за своими словами (не употреблять грубых выражений);

— нельзя сообщать незнакомому лично человеку информацию о себе, своей семье, имена и фамилии родственников, домашний адрес, телефонный номер;

— при дискомфорте в общении нужно выйти из интернета; научите детей доверять интуиции;

— объясните детям, что нельзя открывать файлы, присланные от не известных вам лиц. Эти файлы могут содержать вирусы или фото / видео с агрессивным содержанием;

— относитесь к информации из интернета осторожно. Следуйте правилу трех источников: сравните три разных источника информации, прежде чем решить, каким источникам можно доверять. Не забывайте, что факты, о которых вы узнаете в интернете, нужно хорошо проверить;

— убедите детей в том, что они не должны встречаться с интернет-друзьями в реальной жизни самостоятельно, без взрослых. Скажите, что интернет-друзья могут на самом деле быть не теми, за кого они себя выдают;

— если ваш ребенок получает спам (нежелательную электронную почту), напомните ему, чтобы он не верил написанному в письмах и ни в коем случае не отвечал на них;

— работая в интернете, необходимо сохранять правила человеческого общения. Нравственные принципы в интернете и реальной жизни одинаковы.

Проект решения родительского собрания

1. Учителю совместно с родителями оформить стенд «Родителям на заметку», где будут представлены информация о компьютерных новинках, ссылки на различные развивающие сайты.

2. Обеспечить контроль учителя и родителей за безопасным пребыванием детей в интернете, предпринять необходимые профилактические меры.

Приложение 6

Сценарий родительского собрания по теме «А виноват ли компьютер?»

МБОУ «Школа №105» Н. Новгорода

Аудитория: родители учащихся 5-го класса.

Ход собрания

Вступительное слово учителя:

— Ребенок не может стать игроманом только лишь потому, что в его комнате есть компьютер. Зависимость вызывают не компьютерная графика и не захватывающий сюжет игры, а радость, которую они дарят.

Существует ошибочное мнение, что причина зависимости — наличие компьютера дома. Некоторые родители отказываются покупать ребенку компьютер, чтобы он жил реальной жизнью: учился, гулял, читал, ходил в кружки. Тем самым они наносят удар по его будущей карьере. Сейчас компьютеры везде, и на обочине жизни окажутся те, кто не умеет ими пользоваться. А компьютерную зависимость приобретают далеко не все, для этого нужны предпосылки.

Компьютерные игры — один из способов убежать от действительности. Способ этот не единственный и, пожалуй, наиболее безобидный: по крайней мере, ребенок сидит дома и не очень вредит своему здоровью. Но почему же дети нуждаются в бегстве от действительности?

Разберем ситуацию в нашем классе на основе анонимной анкеты, которая содержит в себе следующие вопросы:

➠ Умеешь ли ты пользоваться интернетом?

➠ Для каких целей ты используешь ресурсы интернета?

➠ Сколько времени ты проводишь в интернете?

➠ Ограничивают ли твое пребывание в интернете родители?

Рассмотрим ответы:

➠ В опросе участвовали 10 девочек и 15 мальчиков, всего 25 человек.

➠ 100 % ответили, что умеют пользоваться ресурсами интернета.

➠ Цели использования интернета: 85 % — игры, 70 % — социальные сети, 75 % — музыка и кино, 35 % — для прикладных увлечений (рисуют, занимаются музыкой и т. д.), 25 % — для учебы.

➠ Время в интернете — от 30 минут в день и до «весь день могу там сидеть».

➠ Только у 65 % опрошенных, по их словам, есть контроль со стороны родителей.

Какой вывод можно сделать?

Узнали вы в ответах ситуацию с вашим ребенком?

«Ты не оправдал ожиданий!»

Павлик был поздним долгожданным ребенком у обеспеченной супружеской пары. Родительские чувства обрушились на Павлика лавиной, а вместе с ними — престижная школа, кружки, частные преподаватели — все самое лучшее и дорогое. Мама упивалась своим поздним материнством, ей хотелось сделать из своего ребенка и музыканта, и спортсмена, и полиглота одновременно. Это все было интересно ей, но не Павлику. Мальчик хотел играть в игрушки, мечтал, чтобы от него отстали. Но нет! День Павлика был расписан по часам, он должен был постоянно исполнять желания матери, которая отыгрывалась на нем за многие годы бездетности.

Раньше Павлик слушался, но в 14 лет произошел срыв. Павлик сел за компьютер и полностью ушел в игры. Слова матери он не воспринимал, она стала для него чужим человеком. В детстве Павлику не дали свободы, внешний мир навалился на него неподъемной тяжестью, задушил домаш-

ними заданиями и обязанностями. Детства как такового не было, и только сейчас, в 14 лет, оно началось. Исполняя мамины желания, Павлик не успел исполнить свои. И теперь он их исполняет! Это желания поиграть, побыть на свободе, избавиться от взрослых проблем. А мать теперь — злейший враг, она мешает ему!

«Спасибо виртуальным монстрам!»

В семье Игоря произошла трагедия. Мать выгнала любимого папу и привела чужого, несимпатичного мужчину. Вскоре у матери родился второй ребенок, и Игорю дали понять, что он в их счастливой семье лишний. Игорь одинок, озлоблен, он запирается у себя в комнате и играет на компьютере в агрессивные игры. И спасибо виртуальным монстрам, которые приняли на себя его негативную энергию, иначе она бы могла обрушиться на людей. Психологи советуют бить подушку, Игорь бьет монстров. Это социально адаптированный выход агрессии! Монстры, как громоотводы, забирают на себя человеческую злость, ненависть, желание убивать и разрушать. Если бы не они, многие подростки выплескивали бы свою агрессию на улице.

Холодный и липкий ужас

У Стасика болеет мать. Она лежит в постели и предрекает страшные вещи: что Стасик скоро останется сиротой, что люди вокруг злы и никто никогда его не пожалеет, что впереди его ждет тяжелая, полная лишений жизнь. Мать стонет, и сын чувствует, что перед ним разверзлась черная, бездонная пропасть. Если бы он мог хоть что-то сделать! Единственное спасение — это компьютер. Там есть веселые наивные мультики, детские игры во всяких рыбок и птичек. Стасику хочется жить в счастливом мире: пусть лучше компьютер станет реальностью, а настоящий мир окажется страшным сном.

Трудности общения

Пятнадцатилетний Миша некрасив, к тому же он инвалид, ходит, прихрамывая. В классе он не котируется, ни одна девушка не обращает на него внимания. Миша избегает об-

щения с людьми и общается только по интернету. Там у него проходит вся жизнь, там и любовь, и дружба, и взаимопонимание.

За компьютером хорошо, а в школе плохо

Виталик плохо учится в школе. Родители постоянно ругают его, угрожают, запугивают. А он, как ни старается, ничего не может изменить: не понимает он математику! Когда Виталик увлекся компьютером, его стали ругать еще больше. «Вместо того чтобы уроки делать, он дурью мается!» Виталик ощущает свою вину, сидя за компьютером, но не может с собой справиться. За компьютером хорошо, а в школе плохо, да и дома с родителями тоже плохо. Компьютер как прекрасный сон, который позволяет отрешиться от внешнего мира!

Вернуть игромана к реальности

Родителям следует задать себе такой вопрос: «Если ребенок перестанет сидеть за компьютером, что в освободившиеся часы он будет делать?» Если в голову придет: «Делать уроки, убираться в квартире», — то их борьба с компьютерной зависимостью бесполезна. Нельзя приятное заменять неприятным, приятное надо заменить еще более приятным, тогда закон физики сработает. Представьте себе, что вы сидите в теплой ванне, а снаружи воздух холодный. Вы пробуете вылезти из ванны, вас обдает холодом, и вы ныряете обратно. Вылезать из ванны хорошо тогда, когда снаружи воздух теплый, не правда ли? Поэтому создайте компьютерным игрокам теплый окружающий мир, который перетянет их на свою сторону!

Как это сделать?

Надо прекратить навязывать ребенку свой сценарий жизни, как это делает мать Павлика, и в то же время не следует превращаться в хнычущего ребенка, как это делает мать Стасика. Родители должны быть сильными и уверенными в себе, готовыми помочь в любой ситуации.

Сам компьютер может предоставить детям нечто более приятное, чем игры: это безграничные возможности для

творчества. Если ваш ребенок только играет, то, вероятно, он плохо знает компьютер. На компьютере можно редактировать фотографии, монтировать собственные фильмы, писать музыку и книги, по-английски общаться с иностранцами. Друг из Великобритании — это отличная практика английского языка!

Конечно, если ваш ребенок развлекается за компьютером вместо того, чтобы делать необходимые дела, это плохо. Рутинный труд неприятен, но он наполняется удовольствием, если человек осознает огромное значение своего труда. Раньше мать в деревне уходила на работу и оставляла старшей дочери все хозяйство и младших детей. Девочке было очень трудно, но она понимала, что ее труд необходим.

Сейчас на детей наваливают обязанности, в которых они не видят смысла. Нынешняя девочка думает: «Почему я обязана читать, если мне это неинтересно? Зачем играть на скрипке, если я не хочу быть музыкантом? Почему надо учить английский? Взрослые хором говорят: “Нужно!” А зачем это нужно, где он применяется?» С точки зрения девочки, ее заставляют делать что-то, лишенное смысла. К тому же она подслушала разговор родителей: «Это надо, чтобы она не болталась на улице!» А она и так «не болтается» на улице, она сидит за компьютером. Поэтому задача родителей — объяснить смысл труда, которым они нагружают своих детей.

Иногда можно наглядно продемонстрировать. Мама попросила сына сходить в магазин, он забыл. Утром он пришел завтракать, а завтрака нет, потому что продукты никто не купил.

Приложение 7

Сценарий родительского собрания по теме «Безопасность наших детей в сети Интернет»

МБОУ «Школа №105» Н. Новгорода

Аудитория: родители учащихся 6-го класса.

Цели:

- повышение уровня знаний о безопасности в интернете;

➠ знакомство с видами опасностей, встречаемых в сети Интернет;

➠ ознакомление с правилами и советами, как уберечь ребенка от риска.

Задачи: познакомить родителей с правилами:

➠ ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет;

➠ критического отношения к сообщениям в СМИ, как отличить достоверные сведения от недостоверных, как избежать вредной и опасной информации, как распознать признаки злоупотребления доверчивостью;

➠ общения в социальных сетях (сетевым этикетом).

Ход собрания

Вступительное слово учителя:

— Отличительной чертой времени, в котором мы живем, является стремительное проникновение информационных технологий во все сферы жизни. Интернет постепенно проникает в каждую организацию, общественное учреждение, учебное заведение, в наши дома. Число пользователей интернета в России стремительно растет, причем доля молодежи и совсем юной аудитории среди пользователей Всемирной паутины весьма велика. Для многих, особенно молодых людей, он становится информационной средой, без которой они не представляют себе жизнь. И это не удивительно: ведь в интернете можно найти информацию для реферата и даже готовый реферат или сочинение, послушать любимую мелодию, купить понравившуюся книгу или обсудить горячую тему на многочисленных форумах. Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями.

Но встретиться с опасностью можно не только в реальном мире — сеть тоже может быть опасна: в ней возникли свои преступность, хулиганство, мошенничество, вредительство и прочие малоприятные явления. Виртуальность общения предоставляет людям с недобрыми намерениями допол-

нительные возможности причинить вред детям. В последнее время в интернете появляется много материалов агрессивного и социально опасного содержания.

Наши дети не исключение, они — активные пользователи интернета.

Иногда именно средства массовой информации, печатные и электронные, оказываются источником угрозы жизни и здоровью людей, в первую очередь детей и подростков. Наверное, вы слышали многочисленные истории о том, как дети становились жертвами преступлений, если вступали в виртуальное общение с незнакомыми людьми, а потом соглашались на встречу с ними. К сожалению, есть случаи, когда старшеклассники оказывались на скамье подсудимых и были осуждены за то, что, уверенные в своей безнаказанности, оставляли в социальных сетях посты, которые позже судом были квалифицированы как экстремистские высказывания.

Учитывая подобные факты и угрозы, Государственная Дума Российской Федерации в декабре 2010 года приняла закон «О защите детей от информации, причиняющей вред их здоровью и развитию». Он вступил в силу с 1 сентября 2012 года.

Также в интернете дети сталкиваются со множеством компьютерных игр, многие из которых могут вызывать зависимость. Как же уберечь ребенка от игровой зависимости? Старайтесь развивать в ребенке другие интересы, кроме компьютерных игр. Секции и студии могут быть любой направленности, главное, чтобы в жизни ребенка появился какой-либо интерес, будь то космос или динозавры, что угодно! Обязательно ходите всей семьей в театры, музеи, кафе, выезжайте на природу, посещайте другие города, чтобы зарядиться новыми впечатлениями и запастись приятными воспоминаниями.

Тест «Определение зависимости от компьютерных игр»

Нужно ответить «да» или «нет». Помните, что от правильности вашего ответа зависят результаты тестирования.

Утверждение	Ответ «да»	Ответ «нет»
Ребенок испытывает затруднения, раздражается, грустит при необходимости закончить компьютерную игру		
Ради компьютерной игры ребенок жертвует времяпрепровождением с семьей, друзьями		
Ребенок преимущественно находится в хорошем настроении, занимаясь компьютерными играми		
Из-за компьютерной игры ребенок пренебрегает сном		
Игра за компьютером — главное средство для снятия стресса у ребенка		
После компьютерной игры у ребенка возникают головные боли		
В обычной жизни ребенок испытывает пустоту, раздражительность, подавленность, которые исчезают при игре за компьютером		
При помощи игры за компьютером ребенок достигает жизненных целей, решает проблемы		
После компьютерной игры у ребенка возникают нарушения аппетита, стула		
Из-за компьютерной игры у ребенка наблюдаются проблемы с учебой (у взрослого — с работой), но он продолжает играть в нее		
Из-за компьютерной игры ребенок пренебрегает питанием		
Ребенок испытывает потребность проводить за игрой все больше времени		
Из-за компьютерной игры ребенок пренебрегает личной гигиеной		
Во время компьютерной игры ребенок полностью отрешается от реальной действительности, целиком переносясь в мир игры		
После компьютерной игры у ребенка возникает сухость слизистой оболочки глаз		

Окончание табл.

Утверждение	Ответ «да»	Ответ «нет»
Из-за компьютерной игры у ребенка появляются проблемы в семье, в отношениях с людьми, но он продолжает играть		
Игра за компьютером служит ведущим средством для достижения комфортного состояния ребенка		

Анализ исследования

За каждый ответ «да» начисляется 1 балл. Если сумма набранных ответов превышает 3 балла, то велика вероятность того, что увлечение ребенком компьютерными играми может перерасти в зависимость, а значит, нужно уже сейчас принимать меры по предотвращению данной зависимости, постараться пробудить у ребенка интерес к чему-то новому и прекрасному, а также можно обратиться к специалистам за психологической помощью.

Риски для детей при пользовании Всемирной паутиной

Контентные риски — это материалы (тексты, картинки, аудио-, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т. д.

Как помочь ребенку избежать столкновения с нежелательным контентом:

➠ Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации подобного рода.

➠ Объясните детям, что далеко не все, что они могут прочесть или увидеть в интернете, — правда. Приучите их спрашивать о том, в чем они не уверены.

➠ Старайтесь спрашивать ребенка об увиденном в интернете. Зачастую, открыв один сайт, ребенок захочет познакомиться и с другими подобными ресурсами.

Коммуникационные риски — такие как незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др.

Даже если у большинства пользователей чат-систем (вебчатов) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы.

Специалисты используют специальный термин «груминг», обозначающий установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

Предупреждение груминга:

- Будьте в курсе, с кем контактирует в интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются.
- Объясните ребенку, что нельзя разглашать в интернете информацию личного характера (номер телефона, домашний адрес, название / номер школы и т. д.), а также пересылать интернет-знакомым свои фотографии.
- Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу.
- Не позволяйте вашему ребенку встречаться с онлайнзнакомыми без вашего разрешения или в отсутствие взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу.
- Интересуйтесь тем, куда и с кем ходит ваш ребенок.

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; со-

циальное бойкотирование с помощью различных интернет-сервисов.

Предупреждение кибербуллинга:

➠ Объясните детям, что при общении в интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов — читать грубости так же неприятно, как и слышать.

➠ Научите детей правильно реагировать на обидные слова или действия других пользователей.

➠ Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

➠ Старайтесь следить за тем, что ваш ребенок делает в интернете, а также за его настроением после пользования сетью.

Даже при самых доверительных отношениях в семье родители иногда не могут вовремя заметить грозящую ребенку опасность и, тем более, не всегда знают, как ее предотвратить.

На что следует обращать внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга:

➠ Беспокойное поведение

Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу — самые явные признаки того, что ребенок подвергается агрессии.

➠ Неприязнь к интернету

Если ребенок любил проводить время в интернете и внезапно перестал это делать, следует выяснить причину. В весьма редких случаях детям действительно надоедает проводить время в сети. Однако в большинстве случаев внезапное нежелание пользоваться интернетом связано с проблемами в виртуальном мире.

➠ Нервозность при получении новых сообщений

Негативная реакция ребенка на звук письма на электронную почту должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Кибермошенничество — один из видов киберпреступления, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации (номера банковских счетов, паспортные данные, коды, пароли и др.) с целью причинить материальный или иной ущерб.

Предупреждение кибермошенничества:

➠ Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в интернете.

➠ Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных.

➠ Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности и, если ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему правила безопасности при совершении онлайн-покупок.

Что делать, если ребенок все же столкнулся с какими-либо рисками

➠ Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и знать, что вы хотите разобраться в ситуации и помочь ему, а не наказать.

➠ Постарайтесь внимательно выслушать рассказ о том, что произошло, понять, насколько серьезно произошедшее и как это могло повлиять на ребенка.

➠ Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или попал в неприятную ситуацию (потратил ваши или свои деньги в результате интернет-мошенничества и пр.), поста-

райтесь успокоить его и вместе с ним разберитесь в ситуации — что привело к данному результату, какие неверные действия совершил сам ребенок, а где вы не рассказали ему о правилах безопасности в интернете.

➠ Если ситуация связана с насилием в интернете по отношению к ребенку, то необходимо получить информацию об агрессоре, выяснить историю взаимоотношений ребенка с ним, понять, существует ли договоренность о встрече в реальной жизни, узнать, были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т. п.). Жестко настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время.

➠ Соберите наиболее полную информацию о происшествии как со слов ребенка, так и с помощью технических средств — зайдите на страницы сайта, где был ваш ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию — в дальнейшем это может вам пригодиться (например, для обращения в правоохранительные органы).

➠ Если вы не уверены в оценке серьезности произошедшего с вашим ребенком, или ребенок недостаточно откровенен с вами или вообще не готов идти на контакт, или вы не знаете, как поступить в той или иной ситуации, — обратитесь к специалисту (телефон доверия, горячая линия и др.), где вам дадут рекомендации о том, куда и в какой форме обратиться.

Общие рекомендации по обеспечению безопасности детей и подростков в интернете

➠ Расположите компьютер вашего ребенка в месте общей доступности: столовой или гостиной. Так вам будет проще уследить за тем, что он делает в интернете.

➠ Следите, какие сайты посещают ваши дети. Если у вас маленькие дети, знакомьтесь с интернетом вместе. Если у вас дети постарше, поговорите с ними о сайтах, которые

они посещают, и обсудите, что допустимо, а что недопустимо в вашей семье. Список сайтов, которые посещает ваш ребенок, можно найти в истории браузера. Кроме того, вы можете воспользоваться инструментами блокировки нежелательного контента, такими как, например, безопасный поиск Google или безопасный режим на YouTube.

- Расскажите детям о безопасности в интернете. Вы не сможете все время следить за тем, что ваши дети делают в сети. Им необходимо научиться самостоятельно пользоваться интернетом безопасным и ответственным образом.
- Установите защиту от вирусов. Используйте и регулярно обновляйте антивирусное ПО. Научите детей не загружать файлы с файлообменных сайтов, а также не принимать файлы и не загружать вложения, содержащиеся в электронных письмах от незнакомых людей.
- Научите детей ответственному поведению в интернете. Помните золотое правило: то, что вы не сказали бы человеку в лицо, не стоит отправлять ему по электронной почте, в чате или размещать в комментариях на его странице в сети.
- Оценивайте интернет-контент критически. То, что содержится в интернете, — не всегда правда. Дети должны научиться отличать надежные источники информации от ненадежных и проверять информацию, которую они находят в интернете. Также объясните детям, что копирование и вставка содержания с чужих веб-сайтов могут быть признаны плагиатом.

Контент-фильтры:

- iProtectYou Pro (http://soft.mail.ru/program_ page.php?grp=5382);
- KidsControl (http://soft.mail.ru/program_ page.php?grp=47967);
- CYBERsitter (http://www.securitylab.ru/software/240522.php);
- КиберМама 1.0b (http://www.securitylab.ru/software/273998.php).

Приложение 8

Методическая разработка родительского собрания по теме «Правила безопасности и этикета в интернете для подростка»

МБОУ «Школа №105» Н. Новгорода

Аудитория: родители учащихся 8-го класса.

Цель: показать родителям важность и значимость проблемы формирования сетевого этикета у подростка.

Задачи:

- актуализировать проблему безопасности детей в сети Интернет;
- побудить родителей задуматься о собственной роли и ответственности за безопасность детей в сети Интернет;
- поддержать положительный опыт семейного пользования интернетом;
- рассказать родителям о правилах общения в интернете.

Вопросы для обсуждения:

- статистика и цифры о роли интернета в жизни школьников;
- влияние интернет-общения на формирование личности ребенка.

Подготовительная работа: анкетирование учащихся, подготовка статистических данных, разработка памяток для родителей и обучающихся, оформление доски.

Ход собрания

Вступительное слово учителя:

— В социальном пространстве информация распространяется быстро благодаря техническим возможностям. Сама информация часто носит противоречивый, агрессивный и негативный характер и влияет на социально-нравственные ориентиры общественной жизни. В связи с этим возникает проблема информационной безопасности, без решения которой не представляется возможным полноценное развитие не только личности, но и общества. Современный школьник, вклю-

ченный в процесс познания, оказывается не защищенным от потоков информации. Пропаганда жестокости средствами массовой информации, возрастающая роль интернета, отсутствие цензуры являются не только социальной, но и педагогической проблемой.

Мы и не думали никогда, что воспитание ребенка будет сопряжено с опасностями, таящимися в интернете.

Интернет-общение в жизни ребенка — это хорошо или плохо? Сколько и как должен общаться ребенок в интернете? Нужно ли ограничивать общение детей в сети? Важно ли прививать этические понятия ребенку по отношения к общению в интернете? На эти и другие вопросы мы постараемся ответить.

Вопросы:

— Чем является компьютер в вашей семье? Приведите примеры ситуаций из вашей жизни, связанных с положительными и отрицательными эмоциями по поводу использования компьютера.

— Что мы сделаем, чтобы не повторять ежедневно: «Ты опять весь день просидел(а) за компьютером»?

— Какую пользу извлекает ваш ребенок при использовании сети Интернет?

— Какие опасности, по вашему мнению, ждут вашего ребенка в сети Интернет?

Результаты анкетирования детей. Анализ, обсуждение ситуаций

Еще недавно компьютеры были скорее роскошью, но уже сейчас являются чуть ли не «предметом первой необходимости». Результаты анкетирования учащихся 5—9-х классов показали, что:

- 90 % детей имеют дома компьютер.
- В среднем ежедневно дети проводят за ним по 4—5 часов в день.
- Из видов деятельности, преобладающих в общении с компьютером, ребята на первое место поставили компьютерные игры. 93 % из них каждый день играют в компьютер-

ные игры, причем 51 % может начать играть, даже не пообедав.

➠ На втором месте — общение в сети. 85 % пользуются интернетом — из них 93 % общаются в социальных сетях, 53 % — играют в сетевые онлайн-игры.

➠ Далее дети выбирают прослушивание музыки, рисование, работу с документами — соответственно 46 %, 13,5 % и 1 %.

➠ 38 % при определении рейтинга использования свободного времени на первое место поставили компьютер, исключив при этом занятия спортом, прогулки на воздухе, общение с семьей.

Достичь высоких результатов в воспитании невозможно без привлечения родителей. Нередко родители недооценивают угрозы, которым подвергается школьник, находящийся в сети Интернет. Комплексное решение поставленной задачи со стороны семьи и школы позволит значительно сократить риски причинения различного рода ущерба ребенку со стороны средств ИКТ. Проблема защиты детей в сети находит самый широкий резонанс. И это не случайно. Интернет может быть прекрасным местом как для обучения, так и для отдыха и общения с друзьями. Но, как и весь реальный мир, сеть тоже может быть опасна. Перед тем как разрешить детям выходить в интернет самостоятельно, следует установить ряд правил, с которыми должен согласиться ваш ребенок. Если вы не уверены, с чего начать, вот десять рекомендаций, как сделать посещение интернета для детей полностью безопасным.

➠ Поощряйте детей делиться с вами их опытом в интернете. Посещайте сеть вместе с детьми.

➠ Научите детей доверять интуиции. Если их в интернете что-либо беспокоит, им следует сообщить об этом вам.

➠ Если дети общаются в чатах, используют программы мгновенного обмена сообщениями, играют или занимаются чем-то иным, требующим регистрационного имени, помогите ребенку выбрать его и убедитесь, что оно не содержит никакой личной информации.

- Настаивайте на том, чтобы дети никогда не выдавали своего адреса, номера телефона или другой личной информации, например места учебы или любимого места для прогулки.
- Объясните детям, что разница между правильным и неправильным одинакова — как в интернете, так и в реальной жизни.
- Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде — даже в виртуальном мире.
- Настаивайте, чтобы дети уважали собственность других в интернете. Объясните, что незаконное копирование чужой работы — музыки, компьютерных игр и других программ — является кражей.
- Скажите детям, что им никогда не следует встречаться с друзьями из интернета. Объясните, что эти люди могут оказаться совсем не теми, за кого себя выдают.
- Скажите детям, что не все, что они читают или видят в интернете, — правда. Приучите их спрашивать вас, если они не уверены.
- Контролируйте деятельность детей в интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и что он делает на них.

В каком возрасте следует разрешить детям посещение интернета?

Дети начинают пользоваться интернетом во все более раннем возрасте. Уже в возрасте семи лет они могут пользоваться интернетом в школе, поэтому, скорее всего, захотят иметь в доступ в сеть и дома. Однако у тех, кто еще не достиг десятилетнего возраста, обычно нет навыков критического мышления, столь необходимого для самостоятельного посещения интернета. Поэтому всякий раз, когда дети выходят в сеть, садитесь рядом и следите за тем, чтобы они посещали только те сайты, которые выбрали вы. Внушите им, что никогда нельзя сообщать в интернете личные сведения.

Следует ли разрешать детям иметь собственные учетные записи электронной почты?

Предпочтительнее, чтобы дети пользовались общим семейным адресом, а не собственным почтовым ящиком. Когда они станут старше и будут настаивать на своей независимости, тогда можно будет завести для них отдельный адрес. Однако корреспонденция может по-прежнему оставаться в семейном почтовом ящике. Это позволит родителям держать под контролем все сообщения, адресованные ребенку.

Какими внутрисемейными правилами следует руководствоваться при использовании интернета?

Выработайте вместе с детьми соглашение по использованию интернета. В нем должны быть описаны права и обязанности для каждого члена семьи, а также четко сформулированы следующие пункты:

- Какие сайты могут посещать дети и что им разрешается там делать.
- Сколько времени ваши дети могут проводить в интернете.
- Что делать, если что-либо вызывает у ваших детей ощущение дискомфорта.
- Как защитить личные данные.
- Как следить за безопасностью.
- Как вести себя вежливо и корректно.
- Как пользоваться службами чатов, группами новостей и мгновенными сообщениями.

Для эффективности такого соглашения крайне важно участие детей в его составлении. Распечатайте его и держите рядом с компьютером для напоминания всем членам семьи, регулярно просматривайте и вносите изменения по мере того, как дети взрослеют. Открытый и доброжелательный диалог с детьми гораздо конструктивнее, чем тайная слежка за ними. В вопросах технологии они всегда будут на шаг впереди вас. Вам лишь необходимо разработать хорошие правила, верить в то, что дети будут их выполнять, и с течением времени вносить в них изменения.

Сетевой этикет

Сетевой этикет — это правила поведения, общения в сети, традиции и культура интернет-сообщества, которых придерживается большинство. Это понятие появилось в середине 80-х годов XX века в эхоконференциях сети FIDO.

Интернет развивается и расширяется, все больше людей общается в сети. Начиная общаться в блогах друг с другом, они допускают множество незаметных на первый взгляд ошибок. Эти ошибки могут доставить неприятности собеседникам в сети. Избежать ошибок помогут несколько советов.

Принципы ведения диалога в социальных сетях

➠ *Принцип вежливого тона*

В ходе общения в сети важно обратиться к партнеру по имени как можно непринужденнее, давая понять, что его имя для вас много значит.

Если вы обращаетесь к кому-либо с просьбой, не забудьте сказать «пожалуйста». В то же время, если кто-то помогает вам, никогда не вредно сказать «спасибо».

➠ *Принцип внимания*

Важное условие успешного ведения беседы в сети — исключительное внимание к собеседнику.

➠ *Принцип рациональности*

Необходимо в ходе диалога в сети вести себя сдержанно, если даже собеседник проявляет эмоции. Неконтролируемые эмоции отрицательно сказываются на процессе общения в сети.

➠ *Принцип понимания*

Постарайтесь понять собеседника в сети. Невнимание к его точке зрения ограничивает возможность выработки различных точек зрения на один вопрос.

➠ *Принцип общения*

Если постоянные читатели не вступают в дискуссию в сети, привлеките их внимание интересной темой.

➠ *Принцип отказа от поучительного тона*

Не старайтесь поучать. Будьте открыты для аргументов и постарайтесь убедить собеседника в необходимости информации.

➠ *Принцип разграничения между собеседником и предметом разговора*

Необходимо разбираться с проблемой, а не друг с другом.

«Смайлики»

Общение в интернете похоже на разговор в реальном времени, но он лишен возможности жестикуляции. Для решения этой проблемы в интернете используются «смайлики» — последовательности ASCII-символов, которые напоминают лицо, если смотреть на них, повернув голову набок.

Чаще всего применяют такие «смайлики»:

:-) или :)- — улыбка; обычно используется для выражения радости, удовольствия (иногда встречается \ или \- — «усмешка»);

:-(или :(- — несчастное лицо; выражает сожаление или разочарование;

;-) или ;)- — подмигивающее лицо; обычно выражает иронию и означает, что слова не следует понимать слишком буквально.

Существуют сотни различных «смайликов», одни используются чаще, другие — реже.

Правильное использование «смайликов» способно придать вашему письму живой характер и даже заменить жестикуляцию. Однако не переусердствуйте.

Подведение итогов

Собрание заканчивается высказываниями детей на тему «Интернет для меня — это…» и выводами родителей: «Мы должны говорить с детьми на тему безопасности и этикета в Интернете…»

Приложение 9
Сценарий классного часа для группы «Юниор-тьютор “ЮнитиК”»
МБОУ «Школа №105» Н. Новгорода

Аудитория: обучающиеся 1—4-х классов.

Цель: ознакомить в игровой форме обучающихся началь-

ных классов с опасностями, которые может таить в себе интернет.

Задачи:

- Подготовить членов группы «Юниор-тьютор “ЮнитиК”» к выступлению.
- Приготовить декорации, провести репетиции по сценарию.
- Провести мероприятие.

Перед младшими школьниками герои мультфильма «Трое из Простоквашино» разыгрывают различные ситуации опасностей, подстерегающих детей в сети Интернет. Затем герои беседуют с детьми. В конце проводится рефлексия, и детям вручаются буклеты с правилами безопасного поведения в сети Интернет.

Сценарий

1-я ситуация

Дядя Федор заходит в дом. Матроскин и Шарик сидят за компьютером. Дома беспорядок, везде паутина, холодно.

Дядя Федор: Матроскин, что тут у вас случилось? Дома беспорядок, холод, паутина…

Матроскин: А мы с Шариком не разговариваем.

Дядя Федор: Почему?

Матроскин: Нам некогда разговаривать. Тут такая компьютерная игра интересная!

Шарик: Ага, мы не можем оторваться.

Дядя Федор: Все понятно. Выключайте компьютер. Будем чай пить с баранками.

Шарик: Дядя Федор, ну можно мы еще немножко поиграем?

Матроскин: Да-да, совсем чуть-чуть! Еще один уровень!

Дядя Федор: Нет! Все, достаточно. Идемте пить чай.

Матроскин и Шарик садятся за стол и пьют чай с виноватыми лицами.

Ведущий: Ребята, давайте скажем Матроскину и Шарику, что они сделали не так. Какая в этом скрыта опасность? Какие советы вы им дадите, чтобы избежать такой ситуации?

Происходит обсуждение.

Матроскин: Мы обещаем, что теперь будем умнее.

Шарик: Будем совмещать приятное с полезным.

2-я ситуация

Сидят Матроскин и Шарик, пьют чай. Стук в дверь.

Шарик: Кто там?

Печкин: Это я, почтальон Печкин. Принес посылку.

Открывают дверь, заходит почтальон Печкин, вручает посылку.

Печкин: От кого эта посылка?

Матроскин: Адрес неразборчивый…

Шарик: Давай быстрей посмотрим, что там.

Открывают посылку — там диск.

Шарик: Ура! Это, наверное, наш Дядя Федор нам компьютерную игру прислал!

Матроскин: А ну, Шарик, включай компьютер, сейчас проверим.

Включают компьютер, загружают диск. Вдруг на экране появляется страшный вирус, пожирающий всю информацию, и экран становится черным.

Шарик и Матроскин сначала пугаются, а потом плачут.

Матроскин: Печкин, давай нам бланк, будем Дяде Федору телеграмму писать.

Ведущий: Ребята, как вы думаете, что им ответит Дядя Федор? А что еще нужно сделать, чтобы уберечь свой компьютер от вирусов?

Происходит обсуждение.

3-я ситуация

Заходят радостные Дядя Федор и Матроскин. Шарик сидит за компьютером.

Матроскин: Шарик, мы нашу Буренку продали, а денежки на сберкнижку положили.

Дядя Федор: В личном кабинете надо пароль придумать.

Шарик: Что тут думать, Дяди Федора дату рождения мы все знаем и не забудем.

Матроскин: Дурак ты, Шарик, это не только мы знаем.

Ведущий: Ребята, но почему Матроскин так сказал? Что тут опасного? Как же быть Дяде Федору?

Происходит обсуждение.

Рефлексия

Матроскин: Ребята, мы разыграли сегодня три ситуации, которые показали опасности сети Интернет.

Шарик: Какие это опасности?

Ведущий: А какие еще опасности таит в себе интернет? Какие правила нужно соблюдать в нем?

Входит Печкин с сумкой.

Печкин: Ребята, наш Дядя Федор прислал вам правила компьютерной безопасности. Сохраните их и старайтесь их соблюдать.

Раздает ученикам буклеты с правилами безопасного поведения в сети Интернет.

Герои прощаются и уходят.

Приложение 10

План-проспект
Недели безопасного интернета
на основе кейс-технологии

МБОУ «Арьёвская школа» Уренского района

Кейс № 1
(для учащихся 1—4-х классов)

Знакомство с проектом «Один день без гаджетов» (ученический проект).

Задание: провести один день без гаджетов, написать сочинение по данной теме или заполнить таблицу «Плюсы и минусы дня без гаджетов».

Кейс № 2
(для учащихся 5—6-х классов)

Комиксы:

- информация о безопасности в сети Интернет (материал сайта http://umnica7.blogspot.ru/2011/08/blog-post_5789.html);

➠ информация о комиксах (буклет).

Задание: создать комиксы по теме «Правила поведения в интернете».

Кейс № 3
(для учащихся 7—8-х классов)

Скрайбинг:

➠ информация о безопасности в интернете (материал сайта http://www.openclass.ru/node/447288);

➠ информация о скрайбинге (буклет);

➠ обучающий практикум (проводит юниор-тьютор).

Задание: создать скрайбинг по теме «Безопасность в сети Интернет».

Кейс № 4
(для учащихся 9—11-х классов)

Сетевой этикет:

➠ найти правила сетевого этикета.

Задание: разместить информацию в облаке в документе совместного пользования.

Акция «Тогда мы идем к вам»

Информация о фильтрах.

Анкетирование родителей о наличии контентной фильтрации.

Установка фильтров на домашние ПК по просьбе родителей (устанавливают волонтеры-старшеклассники).

Акция «День без интернета»

Объявление о предстоящей акции для жителей поселка.

Сбор жителей поселка на площади.

Организация деятельности для создания общепоселковой ледяной горки (снежного городка). ☺

Содержание

Организация безопасной информационной образователь-
О-64 ной среды в образовательной организации : учебно-методическое пособие / авт.-сост. : Е. Г. Калинкина, Ю. Ю. Абышева, Т. И. Канянина, С. Ю. Степанова, И. Н. Лескина, В. Б. Клепиков. — Н. Новгород : Нижегородский институт развития образования, 2018. — 116 с. + 1 электрон. опт. диск.

ISBN 978-5-7565-0759-1

В учебно-методическом пособии представлен практический опыт по созданию безопасной информационной образовательной среды в образовательных организациях, дан обзор законодательной базы и нормативных правовых актов по данной тематике. Использованы материалы конкурса для образовательных организаций, проводимого макрорегиональным филиалом «Волга» ПАО «Ростелеком» и ГБОУ ДПО НИРО при поддержке Министерства информационных технологий, связи и средств массовой информации Нижегородской области.

Учебно-методическое пособие адресовано специалистам органов управления образования, руководителям и педагогам образовательных организаций и направлено на систематизацию работы и распространение успешного опыта по созданию безопасной информационной образовательной среды в школе.

УДК 371
ББК 4313.5я431

Организация
безопасной информационной
образовательной среды
***в* образовательной организации**

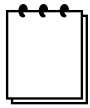
Учебно-методическое пособие

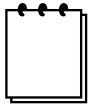
Редактор **Н. Ю. Андреева**
Корректор **В. А. Буренкова**
Компьютерная верстка **Л. И. Половинкиной**

Оригинал-макет подписан в печать 15.06.2018 г.
Формат 60 × 84 $^{1}/_{16}$. Бумага офсетная. Гарнитура «Kudriashov».
Печать офсетная. Усл.-печ. л. 6,98. Тираж 100 экз. Заказ 2475.

Нижегородский институт развития образования,
603122, Н. Новгород, ул. Ванеева, 203.
www.niro.nnov.ru

Отпечатано в издательском центре учебной
и учебно-методической литературы ГБОУ ДПО НИРО





Организация безопасной информационной образовательной среды в образовательной организации

Учебно-методическое пособие

НИРО
НИЖЕГОРОДСКИЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ