Министерство общего и профессионального образования Ростовской области

Государственное бюджетное профессиональное образовательное учреждение Ростовской области «Ростовский-на-Дону колледж связи и информатики»

Е.Л.НОВИКОВА

КИБЕРБЕЗОПАСНОСТЬ

Учебное пособие

г. Ростов-на-Дону
2018 год

Автор:
Е.Л.Новикова, заместитель директора по учебно-методической работе
ГБПОУ РО «РКСИ», к.псх.н.

Рецензент:
Кандидат педагогических наук, Л.В.Упорова.

Новикова Е.Л.
Кибербезопасность. Учеб. пособие для классных руководителей, преподавателей, методистов и руководителей образовательных учреждений. – г.Ростов-на-Дону.: ГБПОУ РО «РКСИ», 2018. – 16 с.

Учебное пособие содержит теоретические основы и рекомендации по кибербезопасности для детей и подростков.

Учебное пособие может быть рекомендовано классным руководителям, преподавателям, педагогам-психологам, методистам и заместителям руководителей и руководителям образовательных учреждений с целью обеспечения кибербезопасности обучающихся.

СОДЕРЖАНИЕ

КИБЕРБЕЗОПАСНОСТЬ

1. АКТУАЛЬНОСТЬ

Вопросы обеспечения информационной безопасности детства являются одной из ключевых проблем детства в современной России.

По различным данным в России каждый день заходит более 80% всех детей, но при этом более 90% процентов сталкивалась с различными проблемами в сети. Можно отметить несколько показательных сведений о российских детях в сети:

- средний возраст начала самостоятельной работы в Сети - 7 лет и сегодня наблюдается тенденция к снижению возраста до 5 лет;
- более 50% процентов детей просматривают сайты с нежелательным контентом;
- более 35% детей посещают порносайты;
- более 60% посещает интернет с развлекательными целями либо для игр.

С каждым годом негативные последствия посещения сети уменьшаются за счет блокировки и не попущения детей до нежелательного и запрещенного контента, активной просветительской работы с детьми и их родителями и увеличения количества пользователей услуг «Родительского контроля» и расширений антивирусных программ.

Так формирование законодательного пространства в части обеспечения информационной безопасности детей началось в 2010 году – с момента принятия Федерального закона от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", последние изменения которого были внесены в мае 2017 года.

В законе понятие информационная безопасность детей определено как состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

К информации, запрещенной для распространения среди детей, относится информация:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;
- отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

– оправдывающая противоправное поведение;
– содержащая нецензурную брань;
– содержащая информацию порнографического характера;
– о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

Оборот такой информации не допускается среди детей в местах, доступных для детей, без применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от такой информации.

Особая категория информация, к которой доступ ограничен для определенных возрастных категорий:

– представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
– вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
– представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
– содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Распространение вышеуказанных категорий информации допускается среди детей определенных возрастных групп при соблюдении обладателем информации установленного законом порядка доступа детей к информации (в частности, при условии, что в информационной продукции содержится идея торжества добра над злом, сострадание к жертве насилия, осуждение насилия, а изображение и описание насилия, жестокости, антиобщественных действий носит ненатуралистический, кратковременный или эпизодический характер и т.п.).

Законом также была закреплена обязанность классификации информации по пяти возрастным категориям:

– информационная продукция для детей, не достигших возраста шести лет;
– информационная продукция для детей, достигших возраста шести лет;
– информационная продукция для детей, достигших возраста двенадцати лет;
– информационная продукция для детей, достигших возраста шестнадцати лет;
– информационная продукция, запрещенная для детей.

Вопросы информационной безопасности детей в дальнейшем были отмечены в качестве приоритета государственной политики детства уже в "Национальной

стратегии действий в интересах детей на 2012-2017 годы", подписанной указом Президента Российской Федерации в 2012 году.

Развитие высоких технологий, открытость страны мировому сообществу привели к незащищенности детей от противоправного контента в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), усугубили проблемы, связанные с торговлей детьми, детской порнографией и проституцией. По сведениям МВД России, число сайтов, содержащих материалы с детской порнографией, увеличилось почти на треть, а количество самих интернет-материалов - в 25 раз. Значительное число сайтов, посвященных суицидам, доступно подросткам в любое время.

Непосредственно обеспечение защиты детей в качестве государственной задачи нашло отражение в разделе «III. Доступность качественного обучения и воспитания, культурное развитие и информационная безопасность детей»: Обеспечение информационной безопасности детства путем реализации единой государственной политики в сфере защиты детей от информации, причиняющей вред их здоровью и развитию

А также в соответствующем подразделе были определены меры, направленные на обеспечение информационной безопасности детства:

Создание и внедрение программ обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет-зависимости, предупреждения рисков вовлечения в противоправную деятельность, порнографию, участие во флешмобах.

Создание правовых механизмов блокирования информационных каналов проникновения через источники массовой информации в детско-подростковую среду элементов криминальной психологии, культа насилия, других откровенных антиобщественных тенденций и соответствующей им атрибутики. Внедрение системы мониторинговых исследований по вопросам обеспечения безопасности образовательной среды образовательных учреждений, а также по вопросам научно-методического и нормативно-правового обеспечения соблюдения санитарно-гигиенических требований к использованию информационно-компьютерных средств в образовании детей.

Создание общественных механизмов экспертизы интернет-контента для детей.

Создание порталов и сайтов, аккумулирующих сведения о лучших ресурсах для детей и родителей; стимулирование родителей к использованию услуги "Родительский контроль", позволяющей устанавливать ограничения доступа к сети "Интернет".

В 2014 году в Совете Федерации прошли парламентские слушания на тему "Актуальные вопросы обеспечения информационной безопасности детей при использовании ресурсов сети Интернет" 14 марта 2014 года, главными итогами которых стали:

– Решение о ежегодном проведении Единого урока по безопасности в сети «Интернет» в образовательных организациях России в октябре;

– Направлении письма Минобрнауки России от 28.04.2014 N ДЛ-115/03 "О направлении методических материалов для обеспечения информационной

безопасности детей при использовании ресурсов сети Интернет" в субъекты Российской Федерации.

Методические рекомендации были направлены на создание в образовательных организациях системы ограничения доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования. Рекомендации содержали рекомендации как технического характера, так и организационного и административного характера.

Так учреждениям рекомендовалось:

– Обеспечить защиту детей от информации, причиняющей вред их здоровью и (или) развитию, посредством использования СКФ, а также путем осуществления педагогами визуального контроля работы детей в сети Интернет;

– Оказать организационную и методическую поддержку работникам образовательной организации, в том числе путем их направления на повышение квалификации по вопросам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, распространяемой посредством сети Интернет;

– Оказать содействие проведению автоматизированного мониторинга использования в образовательных организациях СКФ и мониторинга организационно-административных мероприятий;

– Провести образовательные и консультационные мероприятия с родителями обучающихся с целью объяснения правил, рисков предоставления детям средств связи с выходом в сеть Интернет, в частности, при посещении образовательного учреждения;

– Внести отдельное положение в договор об оказании образовательных услуг, предусматривающего запрет использования личных средств связи с выходом в сеть Интернет или согласие родителей о снятии ответственности с руководителя образовательной организации в случае предоставления своему ребенку данного устройства при посещении образовательного учреждения.

Также органам власти и муниципалитетам рекомендовалось обеспечить повышение квалификации работников образовательных организаций и муниципальных органов управления образованием по вопросам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, распространяемой посредством сети "Интернет".

Следующим важным фактором стало принятие согласно плану мероприятий Национальной стратегии действий в интересах детей Концепции информационной безопасности детей, которая была принята Правительством Российской Федерации 2 декабря 2015 года.

Вопросы организации информационной безопасности в образовательных организациях нашел свое отражение в тексте Концепции:

– Процесс перехода Российской Федерации к постиндустриальному обществу сопровождается последовательной компьютеризацией общеобразовательных организаций и организаций дополнительного образования, иных учреждений для несовершеннолетних, включая детские и юношеские библиотеки. В связи с этим целесообразно предусмотреть внедрение эффективных современных технических и программных средств защиты детей от информации,

причиняющей вред их здоровью, нравственному и духовному развитию, обеспечение соблюдения установленных правил гигиены и безопасности при пользовании компьютерной техникой. Для этого необходимо формирование механизма эффективного использования средств, выделяемых из федерального бюджета и бюджетов субъектов Российской Федерации на компьютеризацию школ и детских библиотек. Вместе с этим необходимо обеспечить в детских и юношеских библиотеках (с сохранением осуществляемых ими в настоящее время функций) медиабезопасность детей, создавая для этого соответствующие технические и организационные условия, а также правовые механизмы.

– Повышение информационной грамотности детей определялась как задача государства и общественных организаций: "Необходима также организация последовательных и регулярных мероприятий государства и общественных организаций, направленных на повышение уровня медиаграмотности детей, которые должны с раннего возраста приобретать навыки безопасного существования в современном информационном пространстве".

– Работа с взрослым населением также была отмечена в качестве приоритета: "Перспективными являются также разработка и внедрение специальных образовательных и просветительских программ, содержащих информацию об информационных угрозах, о правилах безопасного пользования детьми сетью "Интернет", средствах защиты несовершеннолетних от доступа к информации, наносящей вред их здоровью, нравственному и духовному развитию, предназначенных для родителей, работников системы образования, детских и юношеских библиотек и других специалистов, занятых обучением и воспитанием несовершеннолетних, организацией их досуга."

На данный момент федеральными органами исполнительной власти формируется план реализации данной Концепции до 2020 года, которая должна быть представлена до конца 2017 года.

2. ТРЕБОВАНИЯ ФГОС В ЧАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

Федеральный государственный образовательный стандарт основного общего образования в части результатов освоения основной образовательной программы также подчеркивает важность обучения детей навыкам и знаниям обучающихся в сфере информационной безопасности.

Метапредметные результаты освоения основной образовательной программы основного общего образования должны отражать формирование и развитие компетентности в области использования информационно-коммуникационных технологий (далее - ИКТ компетенции) и развитие мотивации к овладению культурой активного пользования словарями и другими поисковыми системами.

Программа развития универсальных учебных действий (программа формирования общеучебных умений и навыков) при получении основного общего образования должна обеспечивать формирование и развитие компетенции обучающихся в области использования информационно-коммуникационных технологий на уровне общего пользования, включая владение информационно-коммуникационными технологиями, поиском, построением и передачей информации, презентацией выполненных работ, основами информационной безопасности, умением безопасного использования средств информационно-коммуникационных технологий (далее - ИКТ) и сети Интернет.

В свою очередь условия реализации основной образовательной программы основного общего образования должны обеспечивать для участников образовательных отношений возможность эффективного использования профессионального и творческого потенциала педагогических и руководящих работников организации, осуществляющей образовательную деятельность, повышения их профессиональной, коммуникативной, информационной и правовой компетентности.

В предметных результатах освоения основной образовательной программы по предметам «Математика. Алгебра. Геометрия. Информатика» ФГОС закрепляет следующее положение: "Формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права".

Конечно же, соответствующие метапредметные результаты и предметные умения отражены в дисциплине «Информатика»:

– требование формирования навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права;

– умения использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;

– понимание основ правовых аспектов использования компьютерных программ и работы в Интернете и т.п.

3. ВИДЫ УГРОЗ

Рассмотрим основные виды информационных угроз, с которыми сталкиваются как дети, так и взрослые.

3.1 Компьютерные вирусы

Компьютерный вирус – это разновидность компьютерных программ, отличительной чертой которой является способность к размножению.

В дополнение к этому, вирусы могут повредить или уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

– Используйте современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;

– Постоянно устанавливайте пачти (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивайте их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включите его;

– Работайте на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;

– Используйте антивирусные программные продукты известных производителей, с автоматическим обновлением баз;

– Ограничьте физический доступ к компьютеру для посторонних лиц;

– Используйте внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;

– Не открывайте компьютерные файлы, полученные из ненадёжных источников.

3.2 Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд WECA, что обозначало словосочетание Wireless Fidelity, который переводится как «беспроводная точность».

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура Wi-Fi. Такое название было дано с намеком на стандарт высший звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работе в общедоступных сетях Wi-fi:

– Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то персональные данные;

– Используйте и обновляйте антивирусные программы и брандмауэр. Тем самым Вы обезопасите себя от закачки вируса на твое устройство;

– При использовании Wi-Fi отключите функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако, некоторые пользователи активируют её для удобства использования в работе;

– Не используйте публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту;

– Используйте только защищенное соединение через HTTPS, а не HTTP, т. е. при наборе веб-адреса вводите именно «https://»;

– В мобильном телефоне отключите функцию «Подключение к Wi-Fi автоматически». Не допускайте автоматического подключения устройства к сетям Wi-Fi без вашего согласия.

3.3 Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты.

Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе необязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

– Ограничьте список друзей. У вас в друзьях не должно быть случайных и незнакомых людей;

– Защищайте свою частную жизнь. Не указывайте пароли, телефоны, адреса, дату рождения и другую личную информацию;

– Если Вы говорите с людьми, которых не знаете, то не используйте свое реальное имя и другую личную информации: имя, место жительства и другие данные;

– Избегайте размещения фотографий в интернете, где Вы изображены на местности, по которой можно определить ваше местоположение;

– При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;

– Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если Вас взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

3.4 Электронные деньги

Электронные деньги — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов – анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификации пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

– Привяжите к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудете свой платежный пароль или зайдете на сайт с незнакомого устройства;

– Используйте одноразовые пароли. После перехода на усиленную авторизацию Вам уже не будет угрожать опасность кражи или перехвата платежного пароля;

– Выберите сложный пароль. Преступникам будет непросто угадать сложный пароль. Надежные пароли — это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т. п. Например, $tR0ng!;

– Не вводите свои личные данные на сайтах, которым не доверяете.

3.5 Электронная почта

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети.

Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена.

Кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

– Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаете и кто первый в рейтинге;

– Не указывайте в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;

– Используйте двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

– Выберите сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

– Если есть возможность написать самому свой личный вопрос, используйте эту возможность;

– Используйте несколько почтовых ящиков. Первый для частной переписки с адресатами, которым Вы доверяете. Этот электронный адрес не надо использовать при регистрации на форумах и сайтах;

– Не открывайте файлы и другие вложения в письмах даже если они пришли от ваших друзей или коллег;

– После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудьте нажать на «Выйти».

3.6 Кибербуллинг или виртуальное издевательство

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

– Не бросаться в бой. Если отвечать оскорблениями на оскорбления, то только еще больше можно разжечь конфликт;

– Управляйте своей киберрепутацией;

– Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;

– Игнорируйте единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;

– Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

3.7 Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало.

Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

– Ничего не является по-настоящему бесплатным. Будьте осторожны, ведь когда предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;

– Необходимо обновлять операционную систему смартфона;

– Используйте антивирусные программы для мобильных телефонов;

– Не загружайте приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

– Периодически проверяйте какие платные услуги активированы на номере;

– Давайте свой номер мобильного телефона только людям, которых Вы знаете и кому доверяете;

– Bluetooth должен быть выключен, когда Вы им не пользуетесь.

3.8 Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься «любимым» делом.

Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей — логинов и паролей. На английском языке phishing читается как фишинг (от fishing — рыбная ловля, password — пароль).

Основные советы по борьбе с фишингом:

– Следите за своим аккаунтом. Если Вы подозреваете, что ваша анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;

– Используйте безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;

– Используйте сложные и разные пароли;

– Если Вас взломали, то необходимо предупредить всех своих знакомых, которые добавлены у Вас в друзьях, о том, что Вас взломали и, возможно, от вашего имени будет рассылаться спам и ссылки на фишинговые сайты;

– Установите надежный пароль (PIN) на мобильный телефон;

– Отключите сохранение пароля в браузере;

– Не открывайте файлы и другие вложения в письмах даже если они пришли от друзей или коллег.

4. ОБУЧЕНИЕ ДЕТЕЙ КИБЕРБЕЗОПАСНОСТИ

Членами и экспертами Временной комиссии Совета Федерации по развитию информационного общества в 2016 году был разработан курс для начального, общего и полного среднего образования межпредметной области «Основы кибербезопасности».

Курс был разработан в соответствии с требованиями и целями ФГОС и Стратегии развития отрасли информационных технологий в Российской Федерации.

Межпредметный курс направлен на внедрение курса по информационной безопасности в учебный процесс разных учебных программ образовательных организаций таких предметов как «Информатика», «ОБЖ», «Биология» и других учебных дисциплин. Тем самым формат межпредметного курса позволит преподавателям различных предметов с учетом своего учебного плана самостоятельно использовать информацию межпредметного курса для расширения кругозора учащихся.

Текст межпредметного курса прошел общественное обсуждение членами Экспертного совета по информатизации системы образования и воспитания при Временной комиссией Совета Федерации по развитию информационного общества.

Межпредметный курс был представлен на парламентских слушаниях «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве», которые пройдут в Совете Федерации 17 апреля 2017 года, а Минобрнауки России рекомендовало включить курс в программы обучения и повышения квалификации педагогических работников.

Курс "Основы кибербезопасности" (https://goo.gl/VJ8ryM) включает:

- Описание целей и задач курса
- Модули курса «Основы кибербезопасности»
- Общие сведения о безопасности ПК и Интернета
- Техника безопасности и экология
- Проблемы Интернет-зависимости
- Методы обеспечения безопасности ПК и Интернета
- Вирусы и антивирусы
- Мошеннические действия в Интернете
- Киберпреступления
- Сетевой этикет
- Психология и сеть
- Правовые аспекты защиты киберпространства
- Государственная политика в области кибербезопасности

Для удобства педагогическим работникам предоставлена информация о учебных модулях в отдельном файле (https://goo.gl/DnjLPo).

Тематическое планирование для курса представлено по следующим предметам: Окружающий мир для 2-4 классов (https://goo.gl/kVneR2); ОБЖ для 5-10 классов (https://goo.gl/EQ7evn); Информатика для 7-11 классов (https://goo.gl/7LGBMr)

Учебное издание

Новикова Елена Леонидовна

КИБЕРБЕЗОПАСНОСТЬ

Учебное пособие