Федеральное государственное автономное образовательное учреждение дополнительного профессионального образования «Академия повышения квалификации и профессиональной переподготовки работников образования»
(ФГАОУ ДПО АПК и ППРО)

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по организации и проведению

ВСЕРОССИЙСКОГО УРОКА БЕЗОПАСНОСТИ ШКОЛЬНИКОВ В СЕТИ ИНТЕРНЕТ
(30 октября)

Авторы:
Семибратов Алексей Михайлович, заведующий кафедрой математики, информатики и информационно-коммуникационных технологий;
Цветкова Марина Серафимовна, доцент кафедры математики, информатики и информационно-коммуникационных технологий

Москва
2017 г.

Аннотация

Методические рекомендации подготовлены в помощь педагогам для проведения и организации Всероссийского урока безопасности школьников в сети Интернет. Методические рекомендации отражают вопросы безопасной работы школьников с информационными и коммуникационными ресурсами сети Интернет для подготовки домашних заданий, доступа к ресурсам для досуга, поиска новостной, познавательной, учебной информации, общения в сети, получения и передачи файлов, размещения личной информации в коллективных социальных ресурсах.

Методические рекомендации адресованы школьным учителям, педагогам дополнительного образования, заместителям директоров по воспитательной работе общеобразовательных учреждений. В основе рекомендаций лежит опыт работы по проведению повышения квалификации работников образования в рамках дополнительных профессиональных программ повышения квалификации, правовые нормы по вопросам информационной безопасности, опыт в области безопасности и рекомендации ведущих ИТ-компаний и мобильных операторов Российской Федерации.

Данные методические рекомендации могут быть использованы учителями информатики, обществознания и права, классными руководителями при работе со школьниками разного возраста в рамках проведения тематических уроков, уроков-дискуссий, бесед, классных часов.

Авторы:

Семибратов Алексей Михайлович, заведующий кафедрой математики, информатики и информационно-коммуникационных технологий;

Цветкова Марина Серафимовна, доцент кафедры математики, информатики и информационно-коммуникационных технологий.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Министерством образования и науки Российской Федерации подготовлен календарь образовательных событий на 2017–2018 учебный год, приуроченных к государственным и национальным праздникам России, памятным датам и событиям российской истории и культуры (письмо «О календаре образовательных событий на 2017/2018 учебный год» Министерства образования и науки Российской Федерации от 02 июня 2017 г. № ТС-134/08). В соответствии с данным письмом разработаны методические рекомендации для общеобразовательных организаций по проведению Всероссийского урока безопасности школьников в сети Интернет.

Безопасность в сети Интернет в свете быстрого развития социальных информационных технологий, их глобализации, использования облачных и мобильных технологий и повсеместного распространения мобильных устройств доступа к сети Интернет, появления большого количества сетевых сервисов и интернет-коммуникаций, в том числе закрытых сетевых сообществ неизвестного толка, а также общедоступных и зачастую навязчивых Интернет-ресурсов (СМИ, реклама), содержащих негативный и агрессивный контент, появление сетевых средств вмешательства в личное информационное пространство на персональных устройствах, работающих в Интернете, массовое использование детьми электронных социальных/банковских карт, имеющих персональные настройки доступа к ним, резко повышает потребность в воспитании у учащихся культуры информационной безопасности в целях предотвращения негативных последствий массового использования Интернета детьми и их защиты от негативной информации.

При реализации требований безопасности в сети Интернет для любого пользователя, будь это школьник или учитель, образовательное учреждение должно обеспечивать защиту конфиденциальных сведений, представляющих собой, в том числе, персональные данные школьника.

Особое внимание необходимо уделять воспитанию у детей культуры информационной безопасности при работе в сети Интернет вне школы. Для этого необходимо проводить непрерывную разъяснительную работу с детьми и родителями, начиная с младшего школьного возраста, формировать у родителей и учащихся ответственное и критическое отношение к источникам негативной информации, в том числе внимательно относиться к использованию детьми личных устройств мобильной связи, домашнего компьютера с Интернетом, телевизора, подключенного к Интернету, использовать дома программные средства защиты от доступа детей к негативной информации или информации по возрастным признакам (возраст+). Научить школьника правильно ориентироваться в большом количестве ресурсов в сети Интернет является немаловажной задачей.

Методические рекомендации освещают основные вопросы защиты школьников в сети Интернет от негативного стороннего воздействия, информирования школьников и их родителей о возможных рисках, которые их подстерегают в сети. Также основной темой методических рекомендаций стали вопросы защиты детей, активно использующих мобильные устройства в сети Интернет, такие как мобильные телефоны с возможностью выхода в сеть Интернет, смартфоны, планшетные устройства и т.д. В методических рекомендациях можно найти подборку полезных ресурсов, которые помогут учителю при составлении материала для проведения тематического урока по безопасности детей в сети Интернет. Такие тематические уроки рекомендуется проводить в виде беседы со школьниками с использованием аудио-визуальных примеров, демонстраций ресурсов, а также подготовив памятки, которые можно использовать как в школе, так и дома.

Особенностью данных методических рекомендаций является проведение урока, посвящённого остро стоящей проблеме безопасного поведения детей в сети Интернет. В свете последних событий в информационном пространстве появились новые угрозы – агрессивный навязчивый контент деструктивного содержания, призывы к агрессии и

террору, что потребовало расширить тему информационной безопасности в сети Интернет такими понятиями, как:

- кибератака,
- киберагент и кибермир,
- киберпреступление,
- кибербезопасность.

С другой стороны, проникновение средств с доступом к Интернету в быт, досуг обострило проблему Интернет-зависимости, игромании, зависимости от социальных сетей.

Новизна методических рекомендаций обусловлена тем, что они подготовлены с учетом этих новых вызовов времени.

В методических рекомендациях по организации и проведению единого Всероссийского урока безопасности школьников в сети Интернет педагоги найдут конкретные предложения по организации инвариантной части Всероссийского урока, посвящённого новым угрозам и новым понятиям информационной безопасности, и по содержанию его вариативной части, которая позволяет учитывать возрастные особенности школьников. Учителям предлагается выбор оптимальных форм проведения урока, рекомендации по использованию информационных образовательных технологий, важнейших средств и приёмов, способов организации информационно-образовательной среды урока или мероприятия, а также предоставлены интересные сведения или ссылки на них, посвящённые сюжетам вариативной части урока (мероприятия).

Цель составления методических рекомендаций: оказать методическую помощь педагогам-практикам в организации и проведении единого Всероссийского урока безопасности школьников в сети Интернет, составить алгоритм подготовки и проведения данного урока в классах различных уровней образования.

Главная цель проведения Всероссийского урока (внеклассного мероприятия) – актуализировать социальные аспекты информационной

безопасности, которые влияют на формирование личностных и метапредметных результатов обучения и воспитания детей.

В соответствии с ФГОС общего образования необходимо сформировать у учащихся такие личностные результаты, которые позволят человеку:

– ориентироваться в информационном мире с учетом имеющихся в нем угроз;

– принимать ценности человеческой жизни, семьи, гражданского общества, многонационального российского народа, человечества;

– быть социально активным, уважающим закон и правопорядок, соизмеряющим свои поступки с нравственными ценностями, осознающим свои обязанности перед семьей, обществом, Отечеством;

– уважать других людей, уметь вести конструктивный диалог, достигать взаимопонимания, сотрудничать для достижения общих результатов;

– осознанно выполнять правила здорового и экологически целесообразного образа жизни, безопасного для человека и окружающей его среды.

В результате отбора содержания урока учитель акцентирует внимание на такие личностные и метапредметные результаты освоения основной образовательной программы общего образования, которые отражают проблематику данного урока:

– освоение социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах, включая взрослые и социальные сообщества; участие в школьном самоуправлении и общественной жизни в пределах возрастных компетенций с учетом региональных, этнокультурных, социальных и экономических особенностей;

– формирование коммуникативной компетентности в общении и сотрудничестве со сверстниками, детьми старшего и младшего возраста,

взрослыми в процессе образовательной, общественно полезной, учебно-исследовательской, творческой и других видов деятельности;

Для учителей информатики и обществознания рекомендуется отразить в содержании урока и некоторые предметные результаты, актуальные для данной темы.

Обществознание:

– формирование основ правосознания для соотнесения собственного поведения и поступков других людей с нравственными ценностями и нормами поведения, установленными законодательством Российской Федерации;

– освоение приемов работы с социально значимой информацией, ее осмысление; развитие способностей обучающихся делать необходимые выводы и давать обоснованные оценки социальным событиям и процессам.

Информатика:

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

Задачи урока (мероприятия):

– формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как ценность человеческой жизни, свободы, равноправия и достоинства людей, здоровья, опыта гуманных, уважительных отношений с окружающими;

– создавать педагогические условия для формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствий деструктивных действий, формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения;

– формировать отрицательное отношение ко всем проявлениям

жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;

– мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально-правовых регуляторов жизни общества и государства в условиях цифрового мира;

– научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны – России в условиях развития цифрового мира, осознавать ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества.

Ожидаемый результат Всероссийского урока: формирование обозначенных в задачах урока личностных, метапредметных и предметных результатов образования в соответствии с требованиями ФГОС НОО, ООО, СОО.

СОДЕРЖАНИЕ МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ

Содержание Всероссийского урока безопасности школьников в сети Интернет решает двуединую педагогическую задачу. В ходе урока, с одной стороны, предполагается освещение правовых, этических, технологических и социально-культурных аспектов обеспечения информационной безопасности детей. С другой стороны, предусматривается более детальное знакомство школьников с новыми вызовами информационного мира, степенью их опасности и способами их предотвращения в соответствии с психолого-возрастными особенностями учащихся по уровням обучения (вариативная часть).

Для предотвращения возможных негативных последствий в случае доступа детей и школьников к неподходящей информации необходимо придерживаться нескольких основных правил:

1. Рассказать детям и школьникам о возможных негативных последствиях, которые могут наступить при работе в сети Интернет.

2. Мотивировать школьников использовать ресурсы сети Интернет для определенных целей.

3. Выстроить беседы с ребенком в максимально доверительном тоне. Доверие между ребенком и взрослым – залог успеха в таком важном деле.

4. Настроить аппаратную защиту – иметь постоянно обновляемый антивирус, поставить программу защиты (контент-фильтр) для сортировки и отсеивания информации негативного характера.

1. ИНВАРИАНТНАЯ ЧАСТЬ УРОКА

Инвариантную часть урока рекомендуется проводить в форме урока-дискуссии. В ходе урока учитель демонстрирует подготовленные материалы, задает вопросы школьникам по заранее подготовленному сценарию, предлагает высказаться на поставленные проблемные вопросы, которые могут быть в ходе дискуссии инициированы школьниками. Итогом такого урока может стать буклет, плакат, листовка о безопасности в сети Интернет, которые будут предложены школьниками для последующих занятий по данной проблематике в классах на уроках обществознания и информатики, на мероприятиях для родителей или выложены на сайте образовательного учреждения для всеобщего ознакомления и информирования школьников и родителей по вопросам безопасности в сети Интернет.

Во вводном слове учитель рассказывает о новых терминах, которые сформировались недавно. Киберне́тика (от др.-греч. Κυβερνητική) – это «искусство управления». Теперь можно говорить не только о безопасности в Интернете, но и о возможности управления информационным пространством в преступных или негативных целях. Достижения науки и техники, создание всемирной сети Интернет позволили преступности выйти на новый уровень и захватить *киберпространство*. Теперь преступнику не нужен прямой контакт с жертвой и всего несколько человек могут стать угрозой для

каждого пользователя «глобальной паутины», крупных корпораций и целых государств.

Конвенцией Совета Европы виды *киберпреступлений* объединены в пять групп.

Первая группа включает все компьютерные преступления, направленные против компьютерных данных и систем (например, незаконный доступ, вмешательство в данные или системы в целом).

Вторую группу составляют противоправные деяния, связанные с использованием технологий (подлог, извлечение, блокировка или изменение данных, получение экономической выгоды иными способами) – мошенничество в Интернете.

Правонарушения третьей группы связаны с содержанием данных или контентом – негативный интернет.

Нарушение авторских и смежных прав (пиратство) относится к четвертой группе, выделение определенных видов преступлений в которой отнесено к законодательству конкретных государств.

Кибертерроризм и использование виртуального пространства для совершения актов насилия, а также другие деяния, посягающие на общественную безопасность, включаются в пятую группу киберпреступлений.

Количество киберпреступлений, совершаемых в мире, неуклонно растет. За последние пять лет их число колеблется в пределах 8 тыс. – 17 тыс., с ежегодной динамикой около 10%. Меняется и их качественный состав, и размер причиненного ущерба. Такое торжество преступности в виртуальном пространстве не может обойтись безнаказанно. Законодательство большинства стран мира предполагает *уголовную ответственность за совершение преступлений данного вида*.

Все эти виды угроз рассматриваются в инвариантной части урока.

Инвариантная часть урока может включать три этапа. На каждом этапе учитель формулирует проблему и доказательно ее описывает. Далее проводится дискуссия по данной проблеме.

Этап 1. Риски, которыми подвергаются школьники в сети Интернет.

В сети Интернет существует немало серьезных рисков, с которыми сталкиваются дети. Получая доступ к информации на сайтах, посвященных преступной деятельности, терроризму и агрессии, или заходя на сайты, подвергающие риску их конфиденциальность, несущие ложную информацию (fake news), дети постоянно находятся в зоне риска сохранности их безопасности и правонарушений. В первую очередь озабоченность вызывает информация, связанная с призывами к агрессии, разрушениям и террористическим действиям, к суициду, видеоматериалы с показом насилия, драк, убийств, порнографии, жестокого обращения с животными, информация с навязыванием деструктивного поведения, правонарушений, неуважительного отношения к людям, реклама алкоголя, курения и другие виды доступной информации, неприемлемой для детей и общества.

Кроме того, дети могут выдать информацию о кредитной карте родителя или ее пароль (а также любые другие пароли), выдать личную информацию о родителях и своей семье, купить вещи без ведома родителей, нарушить авторские права, чем совершить компьютерные преступления, а также получить доступ, передать или стереть личные файлы. В некоторых случаях, они, возможно, даже не знают, что совершают это. Наконец, существует риск атаки личного компьютера вирусами или хакерами.

Вопросы для дискуссии.

Вопрос 1. Какие виды неприемлемой информации попадают под действия Российского законодательства о запрете для распространения?

Рекомендуется обсудить с детьми следующие ответы:

– сайты, посвященные продаже контрабандных товаров или другой незаконной деятельности;

– сайты, подвергающие риску конфиденциальность посетителей;

– сайты с порно-информацией;

– сайты с рекламой табака и алкоголя;

– сайты, посвященные изготовлению взрывчатых веществ;

– сайты, пропагандирующие наркотики; сайты, пропагандирующие насилие и нетерпимость;

– сайты, публикующие дезинформацию;

– сайты, где продают оружие, наркотики, отравляющие вещества, алкоголь;

– сайты, позволяющие детям принимать участие в азартных играх онлайн;

– сайты, на которых могут собирать и продавать частную информацию о самих детях и их семье.

По итогам обсуждения необходимо зафиксировать с детьми возможные пути, приводящие к опасности или рискам при работе в сети Интернет.

Существует несколько типов рисков, с которыми дети могут встретиться, пользуясь Интернетом:

1. Дети могут получить доступ к неподходящей их возрасту информации. К ней относятся: порнография, дезинформация, обман, пропаганда ненависти, нетерпимости, насилия, жестокости.

2. Дети могут получить доступ к информации, совершить действия и купить товары, потенциально опасные для них. Существуют сайты, предлагающие инструкции по изготовлению взрывчатых веществ, продающие оружие, алкоголь, отравляющие и ядовитые вещества, наркотики, табачные изделия, а также сайты, предлагающие принять участие в азартных онлайн играх.

3. Дети могут быть подвержены притеснениям со стороны других пользователей Сети (чаще всего злоумышленниками оказываются другие

дети), которые грубо ведут себя в Интернете, пишут оскорбления и угрожают. Дети также могут загрузить себе на компьютеры вирусы или подвергнуться нападению хакеров.

4. Дети могут выдать важную и личную информацию, заполняя анкеты и принимая участие в онлайн конкурсах и, в результате, стать жертвой безответственных торговцев, использующих нечестные, запрещенные маркетинговые методы.

5. Дети могут стать жертвами обмана при покупке товаров через Интернет, а также выдать важную финансовую информацию другим пользователям (например, номер кредитной карточки, пин-коды и пароли).

6. Дети могут стать жертвой киберманьяков, ищущих личной встречи с ребенком.

Выводы по этапу 1.

Рекомендации для разработки памятки:

– не обращать внимания на звонки и смс, сообщения о выигрышах с незнакомых номеров, никогда не перезванивать на них, не отправлять сообщения;

– никому не сообщать реквизиты своей пластиковой карты, со всеми вопросами обращаться непосредственно в отделение банка;

– установить надежный антивирус на свои устройства и регулярно проводить полную проверку системы;

– покупать только лицензионное программное обеспечение.

Нормативные акты большинства стран мира, в т.ч. и России, предусматривают уголовную ответственность за киберпреступления, при этом наказание варьируется от штрафа до максимальной меры наказания.

Только межгосударственное сотрудничество способно искоренить проблему, и Россия со своей стороны прилагает к этому немалые усилия.

От граждан тоже во многом зависит безопасность киберпространства в целом и их личных данных, средств в частности.

Этап 2. Технологии безопасной работы в сети Интернет.

Для учеников начальной школы рекомендуется дать понятие *компьютерного вируса* и программы *антивирус*. Показать пример антивирусной программы на компьютере, а также показать на компьютере пиктограмму программы-браузера и дать ее понятие – как программы для выхода в Интернет.

Технологии безопасной работы в сети Интернет включают в себя антивирусную защиту компьютера, настройки параметров безопасности для программы браузера.

Вопросы для дискуссии.

Вопрос 1. Почему, находясь в сети Интернет, не нужно терять бдительности и поддаваться ухищрениям злоумышленников (непонятным вам рассылкам по электронной почте, навязчивой рекламе)? (Ответ: это может привести к атаке на персональный компьютер и разрушению информации на нем.)

Вопрос 2. Как нужно построить защиту своего компьютера? (Ответ: установить на нем надежное приложение-антивирус, а также новейшую версию браузера для работы в Интернете с предварительно настроенными параметрами безопасности.)

Залогом безопасной работы в сети Интернет является соблюдение основных правил и рекомендаций, таких как грамотное посещение сайтов и проверка электронной почты. Особенно это становится актуальным при работе на общедоступном компьютере. Обсудите с учащимися правила, мотивируйте из самостоятельно сформулировать каждый из пунктов.

Выводы по этапу 2.

Рекомендуется добавить в памятку следующие пункты для обеспечения безопасности. Безопасность при навигации по сайтам и по приему почты будет достигнута при соблюдении следующих рекомендаций.

1. Установить на своем компьютере антивирусную программу, следить за ее обновлением, реагировать на ее сообщения.

2. Существуют случаи рассылки вирусов, а также вскрытия крупнейших узлов бесплатной почты. Поэтому не исключено, что даже со знакомого адреса может прийти вирус. Если на вашу электронную почту пришло письмо с прикрепленным к нему незнакомым вложением, ни в коем случае нельзя открывать это вложение, а лучше сразу удалить и очистить корзину в программе чтения почты.

3. Никогда не посылать никому свой пароль.

4. При регистрации на сайте необходимо использовать для паролей трудно запоминаемый набор цифр, букв и знаков, причем включить в пароль не менее 6 символов. Об этом часто приходит подсказка при регистрации.

5. Не сохранять свои учетные данные (логин и пароль) для входа в систему на компьютере. После завершения работы с сайтом в Интернете обязательно пользуйтесь функцией завершения сеанса работы с браузером. Просто закрыть окно браузера или ввести другой адрес сайта недостаточно. Это касается и мобильных устройств. Многие программы (особенно программы для обмена мгновенными сообщениями) имеют функцию автоматического входа в систему, сохраняющую имя пользователя и пароль. Отключите эту функцию, чтобы никто, кроме вас, не смог войти в систему.

6. Не оставлять без присмотра компьютер с важными сведениями на экране. Закончив работу на общедоступном компьютере, воспользуйтесь функцией выхода из системы во всех программах и закройте все окна, в которых могут отображаться конфиденциальные данные.

7. Опасайтесь подглядывания через плечо. Работая на общедоступном компьютере или работая с банкоматом, следите за мошенниками, которые подглядывают через плечо, как вы вводите секретные пароли, чтобы потом получить доступ к вашим данным.

Этап 3. Социальные и мобильные сети.

Обсудите с учащимися возможные опасности при работе с соцсетями.

1. **Кибератаки** несут опасность внедрения в учетную запись ребенка. По данным одной из компаний[1], выпускающих антивирусное программное обеспечение: в 53% семей дети-школьники онлайн почти целый день, еще в 22% они посещают Интернет после уроков; 82% детей до 14 лет уже пользуются социальными сетями; 30% родителей понятия не имеют, во сколько их ребенок выходит из сети Интернет ночью. При этом учетные записи в соцсетях – легкая добыча для хакеров. Две трети аккаунтов российских пользователей были взломаны хотя бы один раз, а 21% – неоднократно. Для получения доступа к чужому профилю в соцсети, электронной почте или игровому сервису, злоумышленники могут подобрать пароль. Только 14% респондентов регулярно меняют пароли в соцсетях, 60% делают это от случая к случаю, а 60% – вообще не считают это нужным. Чтобы избежать негативных последствий в соцсетях по взлому аккаунта, необходимо рассказать ребенку о необходимости использования неповторяющихся сложных паролей.

2. **Киберзависимость.** Психологи сравнивают ее с любой другой формой зависимости. Замените слово «компьютер» словами «наркотические вещества» или «алкоголь» – и вы поймете, что Интернет-одержимость вписывается в рамки классического определения зависимости. Она предлагает способ убежать от реальности, приятные чувства и альтернативную реальность, которая маскирует депрессию или беспокойство. Она также может вызвать изменения в нормальном функционировании мозга, стимулируя центры удовольствий.

3. **Киберагенты.** Социальные контакты в Интернете представляют большую опасность, чем телевидение, так как предлагают общение с другими людьми. Общение в Интернете очень привлекательно. Оно полностью анонимно, демократично, доступно и массово. Это чрезвычайно привлекательно, что может приводить к Интернет-зависимости в условиях отсутствия навыков коммуникативной компетентности. Притворяясь новыми

[1] Дети в Интернете - http://www.msk.kp.ru/daily/26405/3281028/

личностями, люди могут начать верить, что их любят и заботятся о них за их новые обличия. Людям нужны друзья, они испытывают потребность принадлежности. Без подобных отношений они могут испытывать серьезные личные и социальные проблемы. Этим пользуются киберагенты, они внедряются в доверие и затем могут оказать негативное психологическое давление на личность ребенка, приводящее к негативным последствиям. Однако способность находить общий язык с людьми вне круга семьи должна воспитываться. Школьная психологическая служба должна быть готова заранее.

4. **Кибермиры.** Помимо того, что виртуальная реальность предлагает легкую альтернативу, она является также соблазнительной заменой, лишенной трудностей социализации, особенно для юных подростков, чья застенчивость может осложнить их социальные отношения. Интернет захватывает ребенка целиком, не оставляя ему ни времени, ни сил на другие виды деятельности, на упорядочивание жизни собственной становящейся личности. Важную роль играет предоставление детям полезных Интернет-ресурсов, творческих состязаний, олимпиад, познавательных сайтов.

5. **Мобильные мошенники.** Сейчас почти у каждого человека есть мобильный телефон. Новое веяние – это подключение услуги доступа в сеть Интернет с мобильного телефона. Ребенок, имея мобильный телефон всегда и везде с собой, бесконтрольно использует его тогда, когда взрослый не может проследить за ним. Также есть риск получения негативной информации и контента путем получения SMS- или MMS -сообщений. Крупные мобильные операторы на своих сайтах дают разного рода рекомендации и предлагают ряд уроков по защите своего мобильного телефона. Около 10 млн. пользователей мобильной связи в той или иной степени пострадали от действий мобильных мошенников. Не только мобильные телефоны, но и различного рода планшетные устройства также нуждаются в защите.

Выводы по этапу 3.

Добавьте рекомендации от компании «Билайн» в памятку:

– Убедитесь в достоверности информации, полученной по телефону от неизвестных, представившихся сотрудниками правоохранительных органов, радиостанции, оператора сотовой связи, чиновниками, вашими родственниками, знакомыми или прочими лицами.

– Не торопитесь предпринимать действия по инструкциям неизвестных людей, полученным посредством телефонного звонка или SMS, в особенности, если их инструкции требуют перевода или передачи вами денежных средств каким-либо способом. Позвоните в Центр поддержки клиентов своего оператора и уточните информацию. Поспешные действия могут привести к финансовому ущербу.

– Уточняйте у оператора стоимость платных номеров, предлагающих участие в акциях и викторинах, проводимых контент-провайдерами.

– Не торопитесь давать телефон на «один звонок» незнакомому человеку. Помните, что в последнее время участились случаи краж телефонов именно таким способом.

– Не открывайте файлы, пришедшие посредством MMS от неизвестных отправителей, а если есть сомнения – то и от известных. По возможности, установите на мобильное устройство одну из многих антивирусных программ.

– Не спешите звонить или отправлять SMS на короткий номер, который обещает разблокировку компьютера от вируса или рекламирует сервис, основанный на доступе к персональным данным других людей. Уточните информацию у своего оператора.

– Для разблокировки компьютера от вирусов используйте антивирусные программы известных разработчиков, в том числе бесплатные версии, размещенные на их сайтах. Не стоит верить сообщениям,

гарантирующим избавление от вируса или исчезновение Интернет-баннера при отправке SMS на короткий номер.

– Вы можете подключить услугу «Черно-белые списки», которая позволяет блокировать доступ к сервисам, предоставляемым контент-провайдерами по Вашему желанию.

2. ВАРИАТИВНАЯ ЧАСТЬ ЕДИНОГО ВСЕРОССИЙСКОГО УРОКА

Для организации вариативной части урока для педагогов полезными будут материалы, которые предлагают ведущие ИТ-компании.

2.1. Уроки безопасного Интернета (компания «Билайн»)

http://moskva.beeline.ru/customers/help/safe-beeline/bezopasnost-detey/v-internete/

Компания «Билайн» проводит информирование пользователей сотовой связи об угрозах, создаваемых мошенниками, использующих средства сотовой связи для обмана людей и получения финансовой выгоды. Для этого создан специальный раздел «**Безопасный Билайн**»[2], в котором особо отметим подраздел «**Дети в интернете**»[3].

Ознакомьте учащихся с этим ресурсом. Предложите выбрать тему для ознакомления с ней учащихся. Время урока указано в минутах.

1. Первая встреча. 5:34
2. Ошибка на сервере – пришлите пароль… 2:45
3. Социальная сеть. 3:46
4. Новый друг. 3:56
5. Антивирусные программы. 4:01
6. Ненужная информация. 3:55
7. Служба мгновенных сообщений. 3:56

[2] http://moskva.beeline.ru/customers/help/safe-beeline/
[3] http://moskva.beeline.ru/customers/help/safe-beeline/bezopasnost-detey/

8. Сплетни и спам. 4:27
9. Поиск. 2:35
10. Платные SMS. 4:35
11. Программы для быстрой работы Интернета. 3:46
12. Компьютерные вирусы. 3:46

Все уроки одним архивом можно скачать по ссылке: http://static.beeline.ru/upload/images/inet_urok_all_10_07_13.rar.

2.2. Урок Дети в Интернете[4] (компания «МТС»)

http://www.safety.mts.ru/ru/deti_v_inete/for_children/lesson/

Компания «МТС» также информирует своих пользователей о разного вида мобильных мошенничествах, о чем сообщает на своем Интернет-ресурсе по адресу http://www.safety.mts.ru/ru/. Ознакомьте учащихся с этим сайтом. Материалы сайта «МТС» будет полезно использовать при составлении памяток для детей об использовании Интернета и мобильных устройств с Интернетом, для работы на классных часах.

На сайте представлены видео[5], урок «**Полезный и безопасный Интернет»**[6], игра «**Необычайные приключения в Интернете»**[7], интерактивная книжка с основными правами поведения в сети Интернет[8].

В специальном разделе для взрослых приведены основные рекомендации по защите детей, использующих мобильные телефоны.

«МТС» предупреждает о видах мошенничества:

– **Дорогие SMS на короткий номер**. Прежде чем отправить сообщение на короткий номер, узнайте его стоимость с помощью бесплатной услуги «Инфоконтент».

[4] http://www.safety.mts.ru/ru/deti_v_inete/for_children/rules/
[5] http://www.safety.mts.ru/ru/deti_v_inete/for_children/video/
[6] http://www.safety.mts.ru/ru/deti_v_inete/for_children/lesson/
[7] http://www.safety.mts.ru/ru/deti_v_inete/for_children/play/
[8] http://www.safety.mts.ru/ru/deti_v_inete/for_children/rules/

– **Кто-то якобы пополнил Ваш счет**. Проверьте, пополнился ли ваш лицевой счет. Помните, что мошенники могут вернуть деньги по чеку в офисе оператора.

– **Мошенники выдают себя за сотрудников банка или сотрудников «МТС»**. Не сообщайте никому свои персональные данные или данные своей банковской карты.

– **Мошенники из Интернета, компьютерные и мобильные вирусы**. Никогда не открывайте сомнительные ссылки в сообщениях или на сайтах. Не открывайте файлы, пришедшие посредством MMS от неизвестных отправителей – это может быть вирус.

– **Мошенники обещают призы**. Не переводите деньги на чужой счет, не вводите никакие коды на своем телефоне и не отправляйте сообщения на короткие номера, если вы не принимали участия в лотерее.

– **Мошенники просят одолжить телефон**. Не одалживайте свой телефон незнакомцам даже «на один звонок» – он может к вам не вернуться.

– **Поздравления от анонима**. Не доверяйте поздравлениям от анонимов, не открывайте открытки от неизвестных лиц – друзья и знакомые вряд ли будут поздравлять анонимно.

– **Фальшивые просьбы о помощи от родных и друзей**. Не доверяйте просьбам о помощи, не убедившись, что они действительно поступают от ваших близких.

Ознакомьтесь с разделом «Сервисы «МТС» для детей и взрослых»[9].

2.3. Курс Академии Яндекс «Безопасность в Интернете»

https://academy.yandex.ru/events/online-courses/internet_security/

Курс включает три блока уроков.

Программа курса:

[9] http://www.safety.mts.ru/ru/deti_v_inete/for_adults/services_mts/

5-6 классы. Защита от вредоносных программ. Мы расскажем о вирусах и других вредоносных программах: как и для чего злоумышленники их используют, как ими можно заразиться и, главное, как избежать заражения.

7-8 классы. Безопасность аккаунтов. Поговорим о том, как и зачем мошенники воруют логины и пароли от электронной почты, социальных сетей и других сервисов. А потом разберем, как уберечь свой почтовый ящик или страницу во ВКонтакте от взлома.

9-11 классы. Безопасные онлайн-платежи. Третья часть посвящена опасностям, связанным с платежами в Интернете. Мы обсудим, как использовать электронный кошелёк или банковскую карту, чтобы не стать жертвой обмана. Рассмотрим основные типы мошенничества и способы от них защититься.

Курс открывается видеороликом.

1. Ознакомьтесь с видеороликом.
2. Пройдите регистрацию
3. Выберите тему для вариативной части урока из предложенных и приступите к обучению.

2.4. Образовательно-выставочный проект «Дети в Интернете»

http://detionline.com/mts/lessons (для 1-4 классов)

Использование данного ресурса на уроке рассчитано на информирование о потенциальных рисках при использовании Интернета, путях защиты от сетевых угроз и полезных возможностях Глобальной сети для образования, развития, общения и досуга. Проект реализуется оператором связи «МТС» совместно с Фондом Развития Интернет при поддержке Министерства связи и массовых коммуникаций Российской Федерации, Министерства образования и науки Российской Федерации, Лиги Безопасного Интернета и ряда партнеров.

Ресурс содержит презентацию для урока и методическое пособие для учителя.

2.5. Специальный раздел Безопасное общение[10] (Компания «Мегафон»)

Основные виды мошенничества, рассматриваемые компанией, – это мошенничество в Интернете[11] и мобильное мошенничество[12].

К мошенничеству в Интернете относятся:

– **«Липовые» акции** – придуманные и обманные акции, с помощью которых мошенники выманивают информацию.

– **Просьба «друзей» сообщить пароль** – друг в социальной сети пишет о потере телефона, просит напомнить ваш номер, вам приходит SMS с неким кодом, а тот же друг в социальной сети сообщает, что заказывает товар или регистрируется на сайте и случайно указал ваш телефон вместо своего. Он просит сообщить пришедший код. Таким образом, ваш номер будет подключен к платной подписке и с вас начнут списывать деньги.

– **Ложная блокировка аккаунта в социальной сети**[13] – на баннере подробно расписан вариант «спасения» от блокирования страницы в социальный сети: отправить SMS на «короткий» номер или ввести код подтверждения, что «Вы не робот». В первом случае происходит разовое списание денег, а во втором оформляется ежедневная подписка на какую-нибудь платную услугу.

– **«Обновление» браузера**[14] – подтверждая загрузку, есть риск подписаться на платную загрузку или получить вирус с архивом платной программы.

---

[10] http://moscow.megafon.ru/bezopasnoe_obschenie/

[11] http://moscow.megafon.ru/bezopasnoe_obschenie/fraud_on_the_internet_social_networks/

[12] http://moscow.megafon.ru/bezopasnoe_obschenie/mobile_fraud/

[13] http://moscow.megafon.ru/bezopasnoe_obschenie/fraud_on_the_internet_social_networks/lock_account_social_network/

[14] http://moscow.megafon.ru/bezopasnoe_obschenie/fraud_on_the_internet_social_networks/update_browser/

– **Фальшивые работодатели**[15] – с помощью поддельного электронного письма пользователя заманивают на сайт, по внешнему виду напоминающий известный и популярный кадровый ресурс. Там соискателю предлагается отправить SMS на «короткий» номер, чтобы якобы зарегистрироваться или получить подходящую вакансию. Соискателя не предупреждают, что цена SMS – несколько сотен рублей, а обещанной информации он, естественно, не получит.

– **Фальшивые антивирусы**[16] – предлагается бесплатный антивирус, под видом которого на устройство попадет вредоносная программа либо создается иллюзия, что компьютер уже заражен и для уничтожения угрозы нужно воспользоваться специальным антивирусом, который, опять же, окажется вирусом.

– **Вирус Trojan. WinLock**[17] – появление надписи на экране компьютера о блокировке операционной системы, устранить которую можно только при отправке SMS с кодом, пришедшим на сотовый при подтверждении, – после чего запускается сам вирус.

Не менее важно знать о мобильном мошенничестве, которое присутствует в различных видах, например:

– Выигрыши, которых не существует[18].

– SMS из несуществующего банка[19].

– Ложные просьбы о помощи, о переводе денег на сотовый[20].

– Требования выкупа[21].

---

[15] http://moscow.megafon.ru/bezopasnoe_obschenie/fraud_on_the_internet_social_networks/phony_employers/

[16] http://moscow.megafon.ru/bezopasnoe_obschenie/fraud_on_the_internet_social_networks/fake_anti-virus/

[17] http://moscow.megafon.ru/bezopasnoe_obschenie/fraud_on_the_internet_social_networks/virus_trojan_winlock/

[18] http://moscow.megafon.ru/bezopasnoe_obschenie/mobile_fraud/winnings/

[19] http://moscow.megafon.ru/bezopasnoe_obschenie/mobile_fraud/sms/

[20] http://moscow.megafon.ru/bezopasnoe_obschenie/mobile_fraud/requests_for_help/

[21] http://moscow.megafon.ru/bezopasnoe_obschenie/mobile_fraud/ransom_demand/

– Wangiri (очень дорогой звонок[22]) – когда кто-то звонит вам с неизвестного номера, но, как только вы берете трубку, звонок внезапно обрывается. Вы перезваниваете на неизвестный номер и попадаете на автоинформатор, задача которого – как можно дольше удержать абонента на линии, пока со счета списываются деньги.

– Выманивание паролей[23].

– Предложения познакомиться[24].

– Ошибочные платежи[25].

– Спам[26].

Также компания ведет раздел для родителей[27], в котором можно найти советы, мобильные уроки для детей и коллекцию добрых сайтов для детей.

Обсудите с учащимися рекомендации, размещенные в этом разделе:

– Вам позвонили или прислали SMS с неизвестного номера с просьбой о помощи близкому человеку:

1. Не впадайте в панику, не торопитесь переводить деньги.
2. Перезвоните родным и узнайте, все ли у них в порядке.
3. Уточните, где находятся близкие, подключите услугу «Маячок».

– Вам позвонили или прислали SMS из «банка» с неизвестного номера:

1. Не впадайте в панику, не торопитесь переводить деньги.
2. Перезвоните родным и узнайте, все ли у них в порядке.
3. Уточните, где находятся близкие, подключите услугу «Маячок».

– Ваш аккаунт в социальной сети заблокирован. Для разблокировки Вас просят отправить SMS на «короткий» номер:

1. Не торопитесь следовать инструкциям.

[22] http://moscow.megafon.ru/bezopasnoe_obschenie/mobile_fraud/wangiri/
[23] http://moscow.megafon.ru/bezopasnoe_obschenie/mobile_fraud/luring_passwords/
[24] http://moscow.megafon.ru/bezopasnoe_obschenie/mobile_fraud/proposals_to_meet/
[25] http://moscow.megafon.ru/bezopasnoe_obschenie/mobile_fraud/erroneous_payments/
[26] http://moscow.megafon.ru/bezopasnoe_obschenie/mobile_fraud/spam/
[27] http://moscow.megafon.ru/bezopasnoe_obschenie/roditelyam/

2. Обратитесь к администрации социальной сети и мобильному оператору.

3. Не доверяйте сомнительным источникам.

4. Не размещайте в социальных сетях конфиденциальную информацию.

– Вам прислали MMS-открытку с неизвестного номера:

1. Не открывайте вложенный файл и не переходите по ссылкам.

2. Удалите сообщение со ссылкой.

3. Защитите свой телефон, подключив бесплатную услугу «Стоп-контент».

4. Используйте антивирусное программное обеспечение для телефонов только от официальных поставщиков.

Все вышеперечисленные операторы мобильной связи имеют обратную форму связи, чтобы любой человек мог сообщить о мошенничестве. Научите школьников ориентироваться в мире безопасного мобильного Интернета, познакомьте родителей с ресурсами основных мобильных операторов – и это будет важным шагом к безопасному общению в сети Интернет.

Итоги вариативной части урока.

Рекомендуется закончить урок информацией об основных законодательных актах в сфере информационной безопасности на основе материалов, размещенных на сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, например, предложить учащимся ознакомиться с памяткой (http://rkn.gov.ru/treatments/p459/p463/?print=1, см. Приложение) или составить листовку в рамках самостоятельной работы на основе изучения материалов:

– персональные данные http://rkn.gov.ru/personal-data/protection-of-the-innocent/;

– контроль и надзор в сфере информационных технологий http://rkn.gov.ru/it/control/;

– контроль и надзор в сфере связи http://rkn.gov.ru/communication/control/;

– контроль и надзор в сфере массовых коммуникаций http://rkn.gov.ru/mass-communications/.

Список источников

1. Роскомнадзор: http://rkn.gov.ru/
2. Безопасный «Билайн»: http://moskva.beeline.ru/customers/help/safe-beeline/.
3. Компания «МТС», раздел по безопасности: http://www.safety.mts.ru/ru/.
4. Безопасное общение, «Мегафон»: http://moscow.megafon.ru/bezopasnoe_obschenie/.
5. Памятка по безопасному общению «Мегафона»: http://moscow.megafon.ru/download/~msk/~moscow/stopfraud/brochure.pdf.
6. Глоссарий по интернет-безопасности: http://ru.norton.com/security-glossary/article.
7. Образовательно-выставочный проект «Дети в Интернете»: http://detionline.com/mts.
8. Курс Академии Яндекс «Безопасность в Интернете»: https://academy.yandex.ru/events/online-courses/internet_security/.

Приложение

Надзор в сфере информационных технологий

Ответы на вопросы в сфере соблюдения законодательства об информационных технологиях.

Вопрос: Имеют ли право администраторы и модераторы сайтов или социальных сетей в одностороннем порядке редактировать записи пользователей, блокировать или удалять страницы пользователей?

Ответ: Как правило, отношения пользователей различных сервисов в информационно-телекоммуникационной сети Интернет, включая социальные сети («ВКонтакте», «Одноклассники», «Мэйл.ру» и другие) и отдельные сайты, носят характер гражданско-правового договора присоединения с администрациями данных сайтов и сетей. Порядок заключения таких договоров регламентирован ст. 428 Гражданского кодекса Российской Федерации. В соответствии с данной нормой условия договора устанавливаются в одностороннем порядке администрацией сайта и содержатся в Пользовательском соглашении (Правилах пользования сайтом).

В соответствии со ст. 428 Гражданского кодекса Российской Федерации и Пользовательским соглашением (Правилами пользования сайта) пользователи сайта могут направить свои обращения, предложения и претензии к администрации сайта. В случае недостижения согласия, споры, связанные с исполнением гражданско-правового договора, разрешаются в судебном порядке по заявлению заинтересованной стороны.

Законом предусмотрено право пользователя на судебное обжалование спорных положений Пользовательского соглашения до заключения договора (до момента регистрации на сайте или в сети). На практике попытки пользователя понудить администрацию сайтов изменить спорные положения Пользовательского соглашения встречаются крайне редко. Пользователи обычно соглашаются с правилами пользования сервисами Интернет-ресурсов.

Надеемся, что по мере развития правовой культуры администраторы и владельцы сайтов будут выдвигать более демократичные условия Пользовательских соглашений, а пользователи научатся защищать свои права в судебном порядке.

Федеральные органы исполнительной власти не имеют права регулировать гражданско-правовые отношения граждан-пользователей и лиц, оказывающих им услуги (администраторов и владельцев указанных сервисов).

Вопрос: Какие меры защиты детей от запрещенной информации могут самостоятельно предпринять родители детей и их воспитатели?

Ответ: В соответствии с ч. 6 ст. 10 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в Российской Федерации запрещается распространение информации, за распространение которой установлена уголовная ответственность.

За незаконное распространение порнографических материалов или предметов (ст. 242, 242.1 УК РФ), а также экстремистских материалов (ст. 280 УК РФ) в Российской Федерации установлена уголовная ответственность.

Борьба с распространением порнографических и экстремистских материалов в сети Интернет находится в сфере ответственности Министерства внутренних дел Российской Федерации.

Однако в настоящее время в законодательстве Российской Федерации отсутствует норма, направленная на запрет распространения информации, пропагандирующей насилие и жестокость по отношению к животным.

Законодательные и исполнительные органы государственной власти осуществляют постоянную систематизацию и совершенствование законодательства Российской Федерации, направленного на пресечение распространения в сети Интернет запрещенной информации.

Минкомсвязь России совместно с другими федеральными органами исполнительной власти разрабатывает проект Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам регулирования отношений при использовании информационно-телекоммуникационной сети Интернет».

Законопроектом предполагается определить субъекты, представляющие услуги в сети Интернет, их функции и отношения, возникающие между ними, ответственность информационных посредников при незаконном распространении информации, а также установить обязанности операторов связи, оказывающих телематические услуги связи.

Одним из вопросов, требующих своего решения в рамках подготовки законопроекта, является определение того, кто, на каких основаниях и по какой процедуре вправе блокировать информацию в сети Интернет.

В целях противодействия распространению в сети Интернет противоправной информации Комитетом Государственной Думы по вопросам семьи, женщин и детей, Комиссией Общественной палаты Российской Федерации по социальной и демографической политике и Общественным советом Центрального федерального округа разработана «Концепция государственной политики в области духовно-нравственного воспитания детей в Российской Федерации и защиты их нравственности».

В рамках реализации указанной Концепции принят Федеральный закон от 29 декабря 2010 г. № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию».

Указанный Федеральный закон регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и развитию, в том числе при обороте информационной продукции, предназначенной для детей, а также устанавливает правовые основы и организационно-правовые механизмы юридической ответственности за невыполнение требований закона.

В данном Федеральном законе закреплены такие успешно апробированные в зарубежной практике правовые механизмы, как осуществляемые на добровольной основе возрастная классификация и предупредительная маркировка информационной продукции, установление ограничений во времени ее теле- и радиотрансляции, иные меры охраны и защиты детей от вредной для них информации.

Федеральный закон от 29 декабря 2010 г. № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию» вступил в силу 1 сентября 2012 года.

Большую работу по выявлению в сети Интернет сайтов с вредоносной информацией выполняют общественные организации. Одной из них является Некоммерческое партнерство «Лига безопасного Интернета». Целями этого общественного объединения являются: полное искоренение опасного контента в сети Интернет, оказание реальной помощи детям и подросткам, которые прямым или косвенным образом стали жертвами распространения опасного контента в сети Интернет, оказание содействия государственным структурам в борьбе с владельцами интернет-ресурсов, занимающимися созданием и распространением опасного контента: детской порнографии, пропаганды наркомании, насилия, фашизма и экстремизма.

О любых противозаконных действия в сети Интернет можно сообщить в эту общественную организацию по адресу: http://www.ligainternet.ru, что позволит оперативно принять меры к устранению возникших проблем.

На ресурсе НП «Лига безопасного Интернета» публикуются материалы, посвященные вопросам противодействия распространению негативного контента в сети Интернет. На сайте представлены рекомендации по безопасному использованию Интернета для различных возрастных групп школьников – младших, средних и старших классов, для родителей, для учителей и преподавателей.

Для работы с компьютером юных пользователей можно использовать специальные браузеры, например MagicDesktop, и Интернет-ресурсы, такие как www.bibigon.ru, www.tirnet.ru, www.gogul.tv, www.telenyanya.ru.

В целях помощи родителям в вопросах безопасного пользования Интернетом государственными органами совместно с крупнейшими операторами связи и общественными организациями проводятся различные мероприятия. Для защиты детей от нежелательного контента в сети Интернет

создано много сервисов, в том числе проект «Дети онлайн» (http://www.DetiOnline.org) . Эксперты проекта помогают детям и консультируют взрослых в ситуациях, связанных с безопасностью несовершеннолетних при использовании Интернета.

На этих сайтах можно познакомиться с большим количеством бесплатных программ по фильтрации контента, с помощью которых родители смогут оградить своих детей от нежелательной информации.

Вопрос: Как защитить свой компьютер от заражения вирусной программой, а себя от мошенничества? (спам, вирусы, SMS-мошенничество)?

Ответ: В сети Интернет получила распространение вирусная спам-рассылка с целью совершения мошенничества с использованием отправки платных SMS-сообщений. Злоумышленники рассылают вредоносные программы, а затем требуют оплатить «лечение» зараженных компьютеров путем отправки платных SMS-сообщений.

Для предотвращения дальнейшего совершения этих преступлений Министерство связи и массовых коммуникаций на своем сайте опубликовало письмо о реализации программы «АНТИ-СПАМ», имеющей целью оказать операторам связи как информационную, так и организационную помощь в защите абонентов от спам-рассылок и мошенничества.

С полным текстом письма можно ознакомиться по адресу: http://www.minkomsvjaz.ru/monitoring-smi/xPages/entry.9556.html.

Однако каждый пользователь Интернет-сети обязан соблюдать определенные правила безопасности.

Пункт 28 Правил оказания телематических услуг связи, утвержденных постановлением Правительства Российской Федерации от 10 сентября 2007 г. № 575, обязывает абонента (пользователя сети):

…б) использовать для получения телематических услуг связи пользовательское (оконечное) оборудование и программное обеспечение, которое соответствует установленным требованиям;

…д) предпринимать меры по защите абонентского терминала от воздействия вредоносного программного обеспечения;

е) препятствовать распространению спама и вредоносного программного обеспечения с его абонентского терминала.

Для предотвращения заражения своего компьютера необходимо следовать простым правилам: никогда не открывать сообщений из неизвестных источников, не распаковывать бесплатно рассылаемых программ, которых Вы не запрашивали, даже если они обещают самую лучшую защиту от вирусов.

Нестандартная ситуация в поведении персональных компьютеров позволяет с большой вероятностью предположить заражение программного обеспечения вредоносной вирусной программой.

Причинами заражения могут быть:

– использование несертифицированного системного программного обеспечения:

– отказ от применения актуализированных программ антивирусной защиты;

– несоблюдение мер безопасности при обращении к сайтам, работа на которых несет повышенную вероятность вирусного заражения (сайты для «взрослых», сайты с размещением фильмов, музыки, студенческих рефератов и т.п.).

В случае заражения компьютера вирусом рекомендуем провести полную проверку актуализированной антивирусной программой и в обязательном порядке удалить из реестра файлов системного обеспечения инфицированные файлы.

За создание программ для ЭВМ или внесение в существующие программы изменений, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование

либо распространение таких программ или машинных носителей с такими программами предусмотрена уголовная ответственность (ст. 273 УК РФ).

Полномочия по борьбе с распространением вредоносных программ и противодействию мошенническим действиям с использованием информационно-телекоммуникационных сетей, включая сеть Интернет, находятся в сфере деятельности Управления «К» Министерства внутренних дел Российской Федерации. О создании, распространении и использовании вредоносных программ и других противоправных действиях в сети Интернет можно сообщить в Общественную приемную МВД России на Правоохранительном портале Российской Федерации: www.112.ru.

Вопрос: Как противостоять размещенным в сети Интернет оскорблениям в свой адрес?

Ответ: В соответствии со ст. 152 Гражданского кодекса Российской Федерации гражданин или юридическое лицо (фирма) вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности. Такая защита допускается только в судебном порядке. Правом обращения в суд наделены исключительно те лица, интересы которых затронуты. Дела рассматриваются судом по месту нахождения ответчика.

Иного порядка защиты чести, достоинства и деловой репутации закон не предусматривает.

Однако, если такие оскорбления сопряжены с распространением заведомо ложных сведений (клеветой), то можно вести речь об ответственности за такие действия в административном порядке.

В соответствии со ст. 5.60 Кодекса Российской Федерации об административных правонарушениях предусматривается ответственность за клевету, т.е. за распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию.

Дела о клевете возбуждаются не иначе как по жалобе потерпевшего, поданной в суд, и в соответствии с ч.1 ст.23.1 КоАП РФ рассматриваются мировым судьей.

Поводами для возбуждения административного дела, в соответствии с п.3 ч.1 ст.28.1 КоАП РФ, являются сообщения и заявления физических и юридических лиц, а также сообщения в средствах массовой информации, содержащие данные, указывающие на наличие события административного правонарушения.