Федеральное государственное автономное образовательное учреждение дополнительного профессионального образования «Центр реализации государственной образовательной политики и информационных технологий» (ФГАОУ ДПО ЦРГОП и ИТ)

Методические рекомендации
по организации и проведению тематических уроков
согласно Календарю образовательных событий, приуроченных
к государственным и национальным праздникам Российской Федерации,
памятным датам и событиям российской истории и культуры

ДЕНЬ ИНТЕРНЕТА. ВСЕРОССИЙСКИЙ УРОК БЕЗОПАСНОСТИ ШКОЛЬНИКОВ В СЕТИ ИНТЕРНЕТ (28–31 октября)

Москва, 2019

АННОТАЦИЯ

Методические рекомендации разработаны в целях оказания методической помощи педагогическим работникам начального, основного, среднего общего образования в организации и проведении «Дня Интернета. Всероссийского урока безопасности школьников в сети Интернет» (28–31 октября).

Данные методические рекомендации адресованы широкому кругу педагогов общеобразовательных организаций: учителям-предметникам, классным руководителям, заместителям директоров по воспитательной работе, социальным педагогам, тьюторам, а также педагогам дополнительного образования и педагогам-библиотекарям.

Предлагаемые материалы могут быть использованы при подготовке тематических уроков и внеурочных мероприятий. Они носят рекомендательный характер, что предполагает их использование с учетом типа образовательной организации, имеющихся материально-технических и информационно-коммуникационных ресурсов, а также интересов, запросов и опыта субъектов образовательного процесса.

Методические рекомендации содержат предложения по подготовке и проведению тематического урока, описание организационной и содержательной составляющих урока, возможных форм организации образовательной деятельности обучающихся, дополнительные материалы для учителя и обучающихся, материалы для работы с родителями, ссылки на тематические ресурсы и рекомендации по их использованию.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Проблема информационной безопасности школьников в сети Интернет – одна из самых актуальных на современном этапе. Интернет уже с раннего возраста становится неотъемлемой частью жизни нового поколения. Имея безграничные возможности для общения, обучения, самовыражения пользователей, интернет-среда оказывает значительное положительное воздействие на развитие детей, обучает и социализирует в увлекательной форме.

Однако Интернет также несет потенциальную возможность вреда для общества, в зависимости от того, как осуществляется его использование.

Дети, захваченные безграничными возможностями современных технологий, зачастую не могут разглядеть рисков и угроз Сети и в результате оказываются среди наиболее уязвимых ее пользователей. Они могут стать жертвой шантажа, вымогательства, манипулирования, оскорблений и нападок со стороны других, потенциальными потребителями негативного интернет-контента (экстремистских материалов различного характера, аддиктивного поведения и зависимостей). А с распространением индивидуальных переносных вычислительных устройств, таких как планшетные компьютеры и смартфоны, риски увеличиваются, так как доступ в Интернет становится переносным и фактически неконтролируемым. Под угрозой оказывается психика ребенка, его образ мышления, жизненные ценности.

Информационная безопасность детей и подростков становится стратегической задачей для государства, так как дети являются его будущим.

Согласно российскому законодательству, информационная безопасность детей – состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Для преодоления отрицательного воздействия сети Интернет на детей в образовательной организации должна быть организована целенаправленная воспитательная работа. Следовательно, каждой образовательной организации необходимо выработать единую стратегию формирования навыков безопасного поведения школьников в Интернете совместными усилиями педагогических работников, родителей и обучающихся.

Работа с обучающимися должна вестись на каждом уровне образования: в начальной, основной и старшей школе. На каждом этапе необходимы специальные формы и методы обучения в соответствии с возрастными особенностями школьников. Формирование навыков

информационной безопасности и сетевой компетентности должно осуществляться не только на уроках информатики, ОБЖ, но и на других предметах и во внеурочной деятельности.

Всероссийский урок безопасности школьников в сети Интернет ежегодно включается в календарь образовательных событий, формируемый Министерством просвещения Российской Федерации.

В соответствии с письмом Министерства просвещения от 27 мая 2019 г. № ТС-1314/04 «О календаре образовательных событий на 2019/2020 учебный год» «День Интернета. Всероссийский урок безопасности школьников в сети Интернет» предлагается провести в образовательных организациях 28–31 октября 2019 года.

Основными *нормативно-правовыми и инструктивно-методическими документами,* определяющими образовательную, воспитательную, организационную деятельность по проведению Всероссийского урока безопасности школьников в сети Интернет, являются:

– Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями и дополнениями);

– Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (с изменениями и дополнениями);

– Указ Президента Российской Федерации от 7 мая 2018 г. № 583 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»;

– Постановление Правительства Российской Федерации от 26 декабря 2017 г. № 1642 «Об утверждении государственной программы Российской Федерации «Развитие образования» (с изменениями и дополнениями);

– Распоряжение Правительства Российской Федерации от 29 мая 2015 г. № 996-р «Об утверждении Стратегии развития воспитания в Российской Федерации на период до 2025 года»;

– Федеральные государственные образовательные стандарты начального, основного, среднего общего образования (с изменениями и дополнениями);

– Рекомендации парламентских слушаний «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве», прошедшие в Совете Федерации Федерального Собрания Российской Федерации 17 апреля 2017 года;

– Приказ Минкомсвязи России от 27 февраля 2018 г. № 88 «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018–2020 годы»;

– Приказ Минкомсвязи России от 29 июля 2018 г. № 330 «О внесении изменения в план мероприятий по реализации Концепции информационной безопасности детей на 2018-2020 годы, утвержденный приказом Министерства связи и массовых коммуникаций Российской Федерации от 27.02.2018 г. № 88»;

– Письмо Минпросвещения России от 27 мая 2019 г. № ТС-1314/04 «О календаре образовательных событий на 2019/2020 учебный год».

Цель методических рекомендаций:

– оказать методическую помощь педагогам в организации и проведении «Всероссийского урока безопасности школьников в сети Интернет».

Задачи методических рекомендаций:

– оказать содействие педагогам в осмыслении актуальности и значимости проблемно-тематического и содержательного поля безопасности школьников в сети Интернет;

– помочь педагогам в отборе и систематизации необходимой информации к уроку;

– предложить педагогам общеобразовательных организаций различные варианты проведения урока с возможностью дополнить мероприятия своими материалами с учетом условий и ресурсов образовательной организации;

– предложить педагогам эффективные подходы к методической, содержательной и технологической составляющей тематического урока с учетом возрастных особенностей школьников, степени их подготовленности к восприятию материала;

– актуализировать необходимость информационной работы по вопросам безопасности школьников в сети Интернет с родителями обучающихся.

СОДЕРЖАНИЕ

Цели тематического урока:

– повышение уровня эрудированности школьников в области интернет-безопасности;

– развитие ключевых компетенций цифровой грамотности у школьников;

– воспитание сетевого этикета и навыков самоконтроля с целью обеспечения информационной безопасности;

– обеспечение внимания родительской и педагогической общественности к данной проблеме.

Для достижения целей решаются следующие **общие задачи тематического урока:**

– ознакомить обучающихся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет;

– помочь учащимся критически относиться к информационной продукции, распространяемой в сети Интернет;

– научить выявлению недостоверных или манипулятивных признаков информации на типичных примерах, распознавать признаки злоупотребления неопытностью и доверчивостью учащихся, попытки их вовлечения в противоправную деятельность;

– обучить избегать информации, способной причинить вред здоровью, нравственному и психическому развитию, чести, достоинству и репутации учащихся;

– познакомить учащихся с нормами и правилами поведения в сети Интернет, основными технологиями противодействия недобросовестной информации.

В то же время необходимо конкретизировать задачи тематического урока по *уровням обучения.*

Для обучающихся начальной школы рекомендуется рассмотреть основные аспекты осуществления деятельности в сети Интернет и меры защиты, с учетом отсутствия у многих детей в данном возрасте собственной электронной почты.

Для обучающихся средней школы вопросы информационной безопасности могут быть расширены за счет изучения психологических и технических аспектов информационной безопасности, вопросов законодательства и ответственности, правил и условий получения, изготовления и распространения информации, получения знаний о мерах защиты, а также знаний источников и принципов работы сетевых рисков.

Для обучающихся старшей школы вопросы информационной безопасности должны быть изучены в той мере, которая позволит самому обучающему стать источником достоверной информации по вопросам информационной безопасности для своих ровесников и младших школьников.

Ожидаемые результаты:

Личностные: формирование мотивации к обучению, навыков социальных и межличностных отношений, ценностно-смысловых установок.

Метапредметные: формирование навыков работы с информацией, умения анализировать и сравнивать, классифицировать и обобщать, делать выводы; освоение навыков различных методов познания, самостоятельной информационно-познавательной деятельности; умений правильно излагать свои мысли в устной и письменной форме, выступать перед аудиторией сверстников, общаться, соблюдая нормы речевого этикета.

Предметные: систематизация и расширение знаний об интернет-безопасности; освоение умений и навыков критической и творческой оценки онлайн-ресурсов, навыков безопасного использования Интернета; освоение этических норм интернет-пользователя; обогащение активного и пассивного словарного запаса, совершенствование видов речевой деятельности.

Всероссийский урок безопасности школьников в сети Интернет для учащихся начальной школы (1-4 классы)

Главная ***цель*** тематического урока в начальных классах – познакомить учащихся с опасностями, которые подстерегают в сети Интернет, и помочь их избежать.

Задачи тематического урока:

– ознакомление младших школьников с правилами ответственного и безопасного поведения в современной информационной среде, способами защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи (тезаурус см. в *Приложении 1*);

– формирование критического отношения к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи, умения отличить достоверные сведения от недостоверных;

– ознакомление с правилами, как избежать вредной и опасной для обучающихся информации, как распознать признаки злоупотребления их доверчивостью и сделать более безопасным свое общение в сети Интернет;

– формирование сетевого этикета: как общаться в социальных сетях, не обижая своих виртуальных друзей, и избегать выкладывания в Сеть компрометирующей информации или оскорбительных комментариев и т.д.

Большое значение для эффективности тематического урока имеет форма его проведения. Выбор форм тематического урока должен осуществляться с учетом таких возрастных особенностей младших

школьников как повышенная эмоциональная возбудимость, быстрая утомляемость, неумение долго концентрировать внимание, желание соревноваться со сверстниками. Поэтому формы занятий должны быть яркими, увлекательными, красочными, привлекать внимание обучающихся своим содержанием, оформлением, новизной и необычностью информации.

Для учащихся 1-4 классов целесообразно использовать беседу, урок-путешествие, урок-викторину, урок-соревнование, урок-сказку, урок-сюрприз, классный час.

Особенно привлекательна для детей младшего школьного возраста урок-***игра***. Для вовлечения детей в процесс игры в материал урока можно вводить сказочные персонажи. Можно использовать конкурс рисунков, тематический рассказ, театрализованное представление.

Большой интерес у младших школьников вызывает творческое задание – ***сочинение сказки***. Если у детей не получается сочинить сказку самим, то можно предложить им самостоятельно придумать начало, конец или продолжение. Самое главное требование к сочинению сказки: сказка должна учить чему-то хорошему («Как Мышонок учился безопасному поведению в сети Интернет», «Сказка о золотых правилах безопасности в сети Интернет»).

Для отбора содержания урока могут быть использованы материалы электронного журнала «Дети в информационном обществе».

Всероссийский урок безопасности школьников в сети Интернет для учащихся основной школы (5-9 классы)

Школьников необходимо познакомить с угрозами мошенничества в Интернете – фишингом и кардингом; научить, как обезопасить себя и что делать, если все-таки попался на удочку мошенников.

Вариантами проведения урока для учащихся 5–9 классов могут стать: создание виртуальной стены; квиз-игра; дискуссия и др.

Одна из форм проведения тематического урока – создание ***«виртуальной стены»*** с помощью ресурса https://padlet.com/. Сайт позволяет создавать виртуальную стенгазету, доску объявлений, сводку новостей или информационный бюллетень.

Цель: уточнить, обогатить и закрепить знания и опыт в области интернет-безопасности.

Педагогу следует заранее зайти на сайт и разобраться в том, что такое «стена», освоить методы работы с программой. Если планируется урок с обучающимися, обладающими высоким уровнем сетевой компетенции,

можно спросить у них, знакомы ли они с данным приложением и смогут ли объяснить классу, как им пользоваться.

Перед началом создания «стены» необходимо обсудить нормы интернет-безопасности, объяснить правила безопасности в Сети.

Учителю необходимо заранее пройти регистрацию на сайте и начать создавать «стену». Затем педагог выводит учащихся на созданную им «стенгазету». Нельзя заполнять всю страницу, достаточно поместить небольшой текст и картинку, после чего предложить классу подумать над тем, чем заполнить свободное пространство.

При создании сетевой стенгазеты выделяются следующие этапы:

1. Совместно принимается решение, какие тексты помещать на газете: только сообщения, или подписи из 140–145 букв, или материалы в другом формате; нужны ли иллюстрации, аудио- и видеоматериалы. Чем младше ученики, тем больше времени они потратят на создание любого материала.

2. Необходимо объяснить учащимся важность взаимоуважения, ответственности за свои слова и поступки, терпимости к иным точкам зрения. Одно из преимуществ виртуальной стенгазеты – возможность не только мгновенно что-то поместить в нее, но и при необходимости убрать пост.

3. Если принято решение об объеме текстов, то нужно проверить, умеют ли школьники пользоваться компьютерным счетчиком. Совместно со школьниками необходимо решить вопросы о числе иллюстраций, их размере, количестве аудио- и видеоматериалов.

Обучающиеся 5-7 классов могут ограничиться составлением предложений, используя новую лексику. Обучающимся 8-9 классов будет интереснее сочинять истории по принципу «буриме», когда каждый придумывает собственные предложения на тему безопасности в сети Интернет. Можно воспользоваться информацией о решении вопросов интернет-безопасности в различных странах мира (см. *Приложение 2*).

4. После того как материалы будут готовы к публикации, необходимо совместно определить порядок их размещения.

5. Если остается время, можно дать детям поиграть, подвигать заметки и картинки, посмотреть, что получается.

Интересной формой проведения занятия является также ***квиз-игра*.**

Цели: сформировать у школьников активную позицию в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им.

Игру можно проводить индивидуально, поделив учеников на группы, или для всего класса. Целесообразно провести ее с помощью компьютеров, планшетов, интерактивной доски и т.д.

Основу квиз-игры составляют вопросы, к выбору которых нужно отнестись ответственно. Слишком простые или сложные вопросы не привлекут внимание обучающихся. Выбирать вопросы могут игроки или учитель. Сложность вопросов может быть одинаковой или меняться в ходе игры. В таком случае, награда за ответ на более сложный вопрос увеличивается. При командном соревновании необходимо обеспечить, чтобы команды не слышали друг друга. К примеру, заполнять промежутки времени между вопросами музыкой.

После завершения игры подсчитываются очки, награждаются победители и призеры. Если проводится серия соревнований в каждой параллели образовательного учреждения, то можно по сумме очков, набранных в играх, составить рейтинг команд. Если игра командная, то можно дополнительно отмечать особо результативных игроков, включив их в отдельный рейтинг.

При проведении квиз-игры можно применить подход, при котором каждый следующий вопрос предлагается при правильном ответе на текущий. Ученику необходимо пройти всю последовательность вопросов и получить максимальное количество очков. Во время ответа на вопрос учащемуся предоставляются дополнительно следующие права:

– заменить вопрос на другой из той же категории сложности;

– воспользоваться помощью эксперта, который предложит свою версию, при этом эксперт может ошибиться, особенно в вопросе высокой сложности;

– один раз за игру застраховать уже выигранную сумму очков (в случае неправильного ответа на вопрос не теряются все очки) и продолжить игру;

– завершить игру и оставить имеющиеся очки, полученные за ответы на вопросы;

– право на одну ошибку – в случае неверного ответа будет еще одна попытка ответить на тот же вопрос.

Рекомендуется провести квиз-игру с ограниченным временем (спринт). Участники за установленное время должны заработать как можно больше очков. Во время спринта ученик или команда играют с обычными правилами. Каждому из игроков или команде предоставляется одинаковый набор вопросов. От учащихся требуется успеть завершить игру до окончания

времени. По окончании игры отображаются все игроки или команды с выигранными ими суммами очков в порядке занятых мест.

Варианты заданий к квиз-игре представлены в *Приложении 4*.

Всероссийский урок безопасности школьников в сети Интернет для учащихся старшей школы (10–11 классы)

Старшеклассникам важно узнать, почему не стоит активно делиться в Сети информацией о своей личной жизни.

Урок целесообразно проводить в таких формах, как круглый стол, квест, брейн-ринг и др.

Круглый стол «Безопасность в сети Интернет»

Цель: сформировать у обучающихся устойчивые навыки работы в сети Интернет.

Уроку предшествует предварительная подготовка. Участники круглого стола заранее знакомятся с темой обсуждения, получают домашнее задание.

Возможные темы круглого стола:

– «Мы в интернет-безопасности»;
– «Мой социум в Интернете»;
– «Безопасность в сети Интернет»;
– «Интернет в современной школе»;
– «Интернет и мое здоровье» и др.

Движущей силой диалога является культура общения и активность слушателей. Большое значение имеет общая эмоциональная атмосфера, которая позволяет вызвать чувство внутреннего единства. Перечень вопросов для обсуждения выявляется посредством анкетирования обучающихся.

Далее учеников следует поделить на группы (5–7 человек). В каждой группе выбирается ведущий, который интервьюирует участников, суммирует и озвучивает мнение каждого участника группы. Желательно, чтобы для каждого вопроса выбирался другой представитель группы. Отдельно можно выделить группу (3–5 человек) экспертов (жюри), которые в ходе урока будут фиксировать выступления каждого участника.

Круглый стол открывает модератор (педагог), который оглашает вопросы, направляет ход обсуждения, следит за регламентом (определяется в начале). По окончании круглого стола подводятся итоги, суммируются конструктивные предложения.

После выступления участника (группы) по одному из вопросов важно организовать общее обсуждение мнений. Необходимо сориентировать

других участников, чтобы они задавали вопросы выступившему. Вопросы могут носить уточняющий характер, а могут содержать контраргумент.

Примерные вопросы для обсуждения на круглом столе представлены в *Приложении 5*.

Еще одной формой проведения урока может стать образовательный ***квест*** **–** специальным образом организованный вид исследовательской деятельности, в итоге которой обучающиеся достигают поставленной заранее цел, выполняя последовательность заданий и следуя правилам.

Например, ***«Квест по информационной безопасности»*** может содержать задания по темам:

– Кибербезопасность.

– Опасности в сети Интернет.

– Персональные данные.

– Кибербуллинг.

Задания можно проходить в любом порядке с любого компьютера.

Примерные вопросы для проведения квеста или брейн-ринга представлены в *Приложении 6*.

Работа с родителями

Для повышения уровня знаний по вопросам обеспечения информационной безопасности детей рекомендуется организовать проведение различных мероприятий с родителями и законными представителями обучающихся.

Такие мероприятия могут проводиться в разных формах:

– родительское собрание, родительский лекторий, заседание родительского клуба на темы: «Основные правила защиты наших детей от интернет-опасностей», «Безопасный Интернет – детям», «Быть или не быть Интернету в компьютере вашего ребенка?»;

– проведение вебинаров с участием экспертов и сотрудников правоохранительных органов по темам: «Важность обеспечения цифровой и информационной грамотности детей и подростков», «Угрозы и риски в сети Интернет», «Методы и функции родительского контроля»;

– демонстрация видеоматериалов по вопросам интернет-безопасности детей;

– анкетирование по вопросам обеспечения защиты детей в информационном пространстве в домашних условиях;

– распространение информационных материалов об обеспечении безопасности детей в сети Интернет: памятки, флаеры и другие материалы

по теме «Советы по обеспечению информационной безопасности детей как особо не защищенных пользователей сети Интернет».

Важно обратить внимание родителей и законных представителей обучающихся на ресурсы российских проектов («Дети России онлайн», «Фонд развития Интернета», «Академия Касперского», «Лига безопасного Интернета», «Безопасность детей в Интернете», проект Google «Сделайте Интернет безопасным для своих детей» и ряд других) и международные программы для подростков (EU Kids Online, Safer Internet Programme), которые дают рекомендации по нормам поведения в сети Интернет и противодействия новым информационным угрозам.

Информация к занятиям представлена в *Приложении 3*.

СПИСОК ЛИТЕРАТУРЫ

1. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010.
2. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК-Пресс, 2017.
3. Данилов О.Е. Роль информационно-коммуникационных технологий в современном процессе обучения // Молодой ученый. – 2013. – № 12. – С. 448–451.
4. Ливингстон С., Блум-Росс А. Только не Инстаграм! // Дети в информационном обществе. – 2016. – № 25. – С. 30–35.
5. Мурсалиева Г. Дети в Сети. Шлем безопасности ребенку в Интернете. – М.: АСТ, 2017.
6. Полезный и безопасный Интернет. Правила безопасного использования Интернета для детей младшего школьного возраста: практическое пособие / под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2017.
7. Поленовский Н.О., Аснина Р. Мальчик в Сети. – М.: Октопус, 2018.
8. Практическая психология безопасности: управление персональными данными в Интернете / Г.У. Солдатова, А.А. Приезжева, О.И. Олькина, В.Н. Шляпников. – М.: Федеральный институт развития образования, 2016.
9. Солдатова Г.У., Олькина О.И. 100 друзей. Круг общения подростков в социальных сетях // Дети в информационном обществе. – 2016. – № 24. – С. 24–33.
10. Солдатова Г.У., Шляпников В.Н. Игры, мультики, учеба // Дети в информационном обществе. – 2014. – № 17. – С. 44–47.

11. Солдатова Г.У., Шляпников В.Н., Журина М.А. Эволюция онлайн-рисков: итоги пятилетней работы линии помощи Дети онлайн // Консультативная психология и психотерапия. – 2015. – Т. 23. – № 3. – С. 50–66.
12. Холловэй Д. От 0 до 8 // Дети в информационном обществе. – 2014. – № 17. С. 24–33.

РЕКОМЕНДУЕМЫЕ ЭЛЕКТРОННЫЕ РЕСУРСЫ

1. Ассоциация электронных коммуникаций (РАЭК) «WWW.I-DETI.ORG»: http://i-deti.org/.
2. Безопасность в Интернете: готовы ли пользователи противостоять киберугрозам?: https://habr.com/en/company/mailru/blog/252091/.
3. «Безопасность детей в Интернете». Информация для родителей: памятки, советы, рекомендации: http://www.ifap.ru/library/book099.pdf.
4. Дети России Онлайн: http://detionline.com/.
5. Детская страница портала «Персональные данные»: http://xn--80aalcbc2bocdadlpp9nfk.xn--d1acj3b/.
6. «Защита детей» – страница на информационном сайте Лаборатории Касперского: https://kids.kaspersky.ru/.
7. Издательство «Образование и Информатика» (ИНФО): http://infojournal.ru/.
8. Интернет-контроль. Сайт для умных родителей: http://www.internet-kontrol.ru/zdorove-detei/zashchita-detei-ot-vrednoi-informatcii-v-seti-internet.html.
9. Информационно-аналитический журнал «Дети в информационном обществе» Фонда развития Интернета: http://www.fid.su/publishing/journal.
10. Комплексный социальный проект «НеДопусти!»: http://nedopusti.ru/site/page/aboutproject/.
11. Компьютерный информационный портал: http://www.oszone.net/6213/.
12. Лига безопасного Интернета: http://www.ligainternet.ru/.
13. Сайт международного конгресса конференций «Информационные технологии в образовании»: https://ito.evnts.pw/.
14. Сценарий урока в библиотеке МЭШ для 5–9 класса по теме «Безопасный Интернет»: https://uchebnik.mos.ru/catalogue/material_view/lesson_templates/369482.
15. Сценарий урока в библиотеке МЭШ для 5–9 и 10–11 классов по теме «Безопасность в сети Интернет»:

https://uchebnik.mos.ru/catalogue/material_view/lesson_templates/445562.

16. Федеральная программа безопасного детского Интернета «Гогуль». http://gogul.tv/.

17. Фонд развития Интернет: http://www.fid.su/. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета.

18. Центр безопасности: https://www.google.ru/safetycenter/families/start/basics/.

19. «Центр безопасного Интернета в России»: http://www.saferunet.ru/.

20. «Центр Интернет-технологий»: https://rocit.ru/.

21. ФГБНУ «Центр защиты прав и интересов детей» – «Твой безопасный кибермаршрут»: https://www.fcprc.ru/projects/cyberbullying.

22. Фонд содействия развитию сети Интернет «Дружественный Рунет»: http://www.friendlyrunet.ru/safety/.

БЕЗОПАСНЫЕ САЙТЫ ДЛЯ ДЕТЕЙ

1. http://web-landia.ru/. – Ресурс лучших сайтов для детей.

2. http://www.microsoft.com. – Информация по безопасности детей в Интернете от Компании Microsoft.

3. http://www.newseducation.ru/. – «Большая перемена»: сайт для школьников и их родителей.

4. www.mirbibigona.ru/ – «Страна друзей»: детская соцсеть: общение, музыка, фотоальбомы, игры, новости.

5. http://www.smeshariki.ru/ – «Смешарики»: развлекательная соцсеть: игры, музыка, мультфильмы.

6. http://www.1001skazka.com – «1001 сказка»: на сайте можно скачать аудиофайлы – сказки, аудиокниги.

7. http://www.nachalka.info/. – Сайт для учащихся начальной школы, а также их родителей и учителей. Здесь можно учиться и играть, развлекаться и закреплять материал школьной программы! Множество упражнений по математике, русскому языку, литературному чтению, окружающему миру не только развлекут ребенка, но и помогут закрепить навыки, требуемые в рамках федерального государственного образовательного стандарта.

8. http://www.teremoc.ru. – Детский сайт «ТЕРЕМОК» с развивающими играми, загадками, ребусами, мультфильмами.

9. http://www.murzilka.org/. – Сайт журнала «Мурзилка» со стихами, раскрасками, конкурсами и другой полезной информацией.

ПРИЛОЖЕНИЯ

Приложение 1.

Тезаурус темы

Вирус (вредоносная программа) – это любое программное обеспечение, используемое для получения несанкционированного доступа к информации или ресурсам компьютера с целью хищения, удаления, искажения или подмены данных. Вирусы делятся на группы по типу заражаемых объектов, методам заражения и жертвам. Заразить компьютер вирусом можно разными способами: от использования съемного носителя до посещения вредоносного сайта. Благодаря антивирусным компаниям в наше время вирусы встречаются довольно редко.

Интернет-безопасность – это отрасль компьютерной безопасности, связанная специальным образом не только с Интернетом, но и с сетевой безопасностью, поскольку она применяется к другим приложениям или операционным системам в целом. Ее цель – установить правила и принять меры для предотвращения атак через Интернет. Интернет представляет собой небезопасный канал для обмена информацией, который приводит к высокому риску вторжения или мошенничества, таких как фишинг, компьютерные вирусы, «трояны», «черви» и многое другое.

Интернет-культура (англ. Internet culture) – культура подачи информации и культура общения пользователей в Интернете, которая возникла благодаря Интернету и стала глобальным феноменом.

Информационная гигиена, информационная экология – составные части информационной безопасности. Раздел медицины, изучающий закономерности влияния информации на психическое, физическое и социальное благополучие человека, его работоспособность, продолжительность жизни, общественное здоровье социума, разрабатывающий нормы и меры по оздоровлению окружающей информационной среды и оптимизации интеллектуальной деятельности.

Кардинг (мошенничество с банковскими картами) (от англ. carding) – вид мошенничества, при котором производится операция с применением платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Обычно реквизиты банковских карт берут с взломанных серверов интернет-магазинов, платежных и расчетных систем, а также с персональных компьютеров (непосредственно

или через программы удаленного доступа, «трояны», «боты» с функцией формграббера).

Кибербуллинг (электронная травля) – это вид преследования, преднамеренные агрессивные действия систематически на протяжении долгого периода времени, осуществляемые лицом или группой лиц с использованием электронных форм взаимодействия, направленных против жертвы, которая не может себя защитить. Это может происходить через СМС-сообщения, социальные сети, создание компрометирующих веб-страниц или размещение унижающих, оскорбляющих видео, фотоматериалов и др.

Киберпространство (англ. cyberspace) – метафорическая абстракция, используемая в философии и в компьютерных технологиях, является виртуальной реальностью, которая представляет Ноосферу. Второй мир как «внутри» компьютеров, так и «внутри» компьютерных сетей.

Персональные (личностные) данные – сведения, относящиеся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), которые предоставляются другому физическому или юридическому лицу либо лицам.

Редирект – процесс автоматического перенаправления посетителя с одного сайта на другой, который можно настроить для отдельных и для всех страниц, каталогов, разделов.

Спам (англ. spam) – массовая рассылка назойливых рекламных писем лицам, не соглашавшимся их получать.

Цифровая безопасность – основы безопасности в сети Интернет. Включает в себя защиту персональных данных, надежный пароль, легальный контент, культуру поведения, защиту репутации, сетевой этикет, безопасное хранение информации, создание резервных копий.

Цифровая грамотность – набор знаний и умений, которые необходимы для безопасного и эффективного использования цифровых технологий и ресурсов Интернета. Включает в себя цифровое потребление; цифровые компетенции; цифровую безопасность.

Цифровые компетенции – навыки эффективного пользования информационно-коммуникационными технологиями.

Цифровое потребление – использование Интернета для работы и жизни.

Фишинг (англ. phishing, искаженное «fishing» – «рыбалка») – вид мошенничества в Интернете. Целью является получение доступа к конфиденциальным данным пользователей (логинам и паролям).

Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. Также мошенники могут создать сайт, который будет внушать доверие пользователю, например – сайт, похожий на сайт банка пользователя, через который и происходит похищение реквизитов платежных карт. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам. Наиболее распространенный метод похищения номеров платежных карт.

Формграббер (от англ. form grabbing – захват формы) – шпионская программа, служит для перехвата введенных паролей и логинов. Механизм заполнения формы (с клавиатуры, перетаскиванием, копированием, автоматически средствами браузера) не влияет на работу формграббера. Перехват данных не изменяет функционирование основной системы, введенная пользователем информация корректно передается и обрабатывается.

Приложение 2.

Информация об интернет-безопасности детей в разных странах мира

Великобритания. В борьбу за безопасный Интернет Великобритания включилась с конца 1990-х годов. Интернет-провайдеры британских телекоммуникаций предоставляют интернет-трафик с использованием услуги «Чистая линия», которая блокирует нежелательный контент.

Осенью 2017 года министр культуры Великобритании Карен Брэдли предложила ввести «общенациональный сбор», посредством которого социальные сети и поставщики услуг займутся финансированием программ повышения осведомленности об опасностях Интернета. Предполагается, что социальные мессенджеры будут раскрывать информацию о размерах распространения ксенофобии и агрессии, для того чтобы имелась возможность противодействовать подобным случаям.

Политик призвала ввести добровольный «этический кодекс» и как можно быстрее удалить любые жестокие материалы, направленные на разжигание ненависти. Социальные сети должны нести ответственность

за контент, а правительствам необходимо научиться решать проблемы, возникающие в Сети. Предотвращение кибербуллинга в Интернете должно стать незаменимой составляющей школьного образования.

По данным отчета Национального общества защиты детей от жестокого обращения (NSPCC), в Великобритании в 2016–2017 гг. проведено 12248 консультаций ChildLine, посвященных безопасности и злоупотреблениям в Интернете, – на 9% больше, чем в предыдущий период.

Франция. Весной 2011 года министр образования Франции постановила: интернет-преследователи должны быть идентифицированы и при соответствующих обстоятельствах освобождены от занятий или даже исключены из школы. Учителя обязаны вести учет контента блогов. С 1 сентября 2018 года ученикам начальных и средних школ Франции запрещено приносить в учебные заведения гаджеты, подключенные к Интернету. Руководители лицеев, куда приходят обучающиеся старше 15-летнего возраста, будут решать, запрещать гаджеты или нет, самостоятельно; гражданам до 16 лет запрещено заводить аккаунты в социальных сетях без родительского согласия.

Германия. В Германии кибербуллинг не имеет статус преступления, но отдельные его стороны преследуются законом. Интернет-травля в Германии причисляется к деликту – частному или гражданско-правовому проступку, влекущему за собой наказание для взрослых до 10 лет лишения свободы. Обычно подростки подвергаются меньшему наказанию – до 5 лет лишения свободы или принудительным исправительным работам. Существует закон «О защите прав молодого поколения», в котором имеются параграфы, которые регулируют использование социальных медиа.

Европейский Союз. Создана программа «Безопасный Интернет», задачи которой поддержка и защита детей и молодых людей в режиме «горячей линии» путем реализации инициатив повышения осведомленности и борьбы с незаконным и деструктивным контентом и поведением в Интернете. В 2004 году создано Европейское агентство сетевой и информационной безопасности ENISA.

США. В 1998 году в стране принят закон «О защите неприкосновенности частной жизни детей» (начал действовать с 21 апреля 2000 года). Закон регулирует отношения, возникающие в связи со сбором в Интернете физическими или юридическими лицами персональных данных у детей младше 13 лет (для получения информации от детей необходимо разрешение родителей или опекунов). В 2000 году

принят закон «О защите детей в Интернете», который обязал школы и библиотеки установить блокирующие программы и специальные фильтры в сети Интернет.

В 2008 году в штате Миссури введен закон, направленный на противодействие кибербуллингу. Закон принят после вызвавшего широкий общественный резонанс самоубийства подростка. В штате Нью-Джерси после суицида студентки были приняты строгие законы против кибербуллинга в школе и в ВУЗах.

Весной 2011 года в Белом доме состоялась встреча на высшем уровне, посвященная противодействию интернет-травле. На встрече представители Facebook объявили, что планируют создать отдел медиации по спорам.

Приложение 3.

Информация и советы для родителей

Дети поколения Z активно используют мобильные устройства, создают сетевые сообщества и пользуются различным информационным контентом. Социальные сети сделали процесс загрузки контента простым, большинство несовершеннолетних ищет в Интернете готовое содержимое, рассчитанное на широкую публику. Проблема контакта с размещенным в Сети нежелательным, негативным контентом является одной из самых острых.

Родителей необходимо поощрять использовать больше способов контроля, для этого необходимы простые и доступные в использовании специальные инструменты.

Поскольку несовершеннолетние все чаще пользуются Интернетом частным образом или с помощью мобильных устройств, совет поместить компьютер в общую комнату уже не актуален. 53% пользователей выходит в Интернет из дома друзей, 49% – из собственной комнаты, а 33% – при помощи мобильного телефона или иного устройства. Поэтому родителям лучше беседовать об Интернете с детьми и даже практиковать совместные виды деятельности.

Столкнуться с риском – еще не означает пострадать. Родителям стоит больше беспокоиться о том, чтобы их дети не пострадали, а не бороться с риском. Необходимо направлять детей при любой возможности, это поможет избежать ущерба или компенсировать его. Родители должны быть в курсе редких, но травмирующих инцидентов, произошедших у детей (включая подростков) в Интернете.

38% пользователей в возрасте от 9 до 12 лет имеют собственный профиль в социальных сетях. Возрастные ограничения не работают. Даже если поставщик услуг разработал бы специальные настройки безопасности для несовершеннолетних, это было бы бесполезно, поскольку многие малолетние пользователи при регистрации указывают неверный возраст. Некоторые участники размещают свои персональные данные в профиле, другие общаются с людьми, которых раньше не встречали.

Четыре из десяти пользователей контактируют с людьми, с которыми познакомились в Интернете, но эти люди связаны с их друзьями или родственниками. Четверть общается с кем-то, кто не связан с их социальным окружением, а 9% встречались в реальной жизни с теми, с кем познакомились в Интернете.

Частично подтверждается то, что несовершеннолетние, которые сталкивались с разными опасностями в реальной жизни, с большей долей вероятности повторят этот опыт в Интернете и могут пострадать от этого. Но встреча с опасностями в реальности не означает, что в виртуальном мире риски обязательно появятся, и не стоит полагать, что, если ребенок не рисковал в реальной жизни, он будет в безопасности в Интернете.

Всего 28% пользователей в возрасте 11–16 лет признаются, что умеют изменять настройки фильтра. Большинство считает, что действия родителей в отношении использования сетевых ресурсов оказываются полезными. Однако почти половина действительно считает, что действия родителей ограничивают их деятельность в Интернете, а одна треть утверждает, что игнорирует мнение родителей.

Более совершенные технические навыки связаны с большей, а не с меньшей степенью риска. Больше активность – лучше навыки, лучше навыки – больше возможностей, больше возможностей – больше риска. Одна из причин взаимосвязи возможностей и рисков заключается в том, что дети должны подвергаться риску в определенной степени, это научит их восстанавливать душевное равновесие. Другой момент заключается в том, что поиск информации или развлечений приводит к непредвиденной опасности, поскольку виртуальный мир создавался без учета интересов несовершеннолетних (к примеру, в нем слишком много всплывающих окон). Но развитые навыки могут помочь уменьшить ущерб, нанесенный Интернетом.

ПРИЛОЖЕНИЕ 4.

Примерные вопросы к квиз-игре

Что делать в случае, если приходится заходить в аккаунт через компьютер друга? Варианты ответов.

1. Попросить друга не смотреть, как вы вводите пароль.

2. *Не нажимать галочку «Запомнить пароль», а также почистить историю после завершения сессии или включить в браузере режим «инкогнито».*

3. Компьютер друга такой же безопасный, как собственный, поэтому можно ничего не предпринимать.

Вы нашли объявление, в котором предлагается выполнить легкую работу за большое вознаграждение, но заплатят лишь после выполнения работы. Как правильно поступить в таком случае? Варианты ответов.

1. Срочно откликнуться, пока кто-нибудь вас не опередил.

2. Связаться с работодателем и согласиться на работу при условии, что он пришлет вам письмо с гарантией оплаты.

3. *Не откликаться на вакансию.*

Что чаще всего интересует злоумышленников в Интернете? Укажите один или несколько правильных вариантов ответа.

1. Фотографии на компьютере и телефоне.

2. *Данные банковских карт и счетов.*

3. *Список контактов для рассылки спама от чужого имени.*

Браузер предупреждает, что сайт, на который вы хотите перейти, заражен вирусом. Ваши действия? Укажите правильный вариант ответа.

1. Все равно перейду на сайт, так как браузер не может такого знать.

2. Перейду на сайт, потому что браузер не антивирус.

3. *Не стану переходить на сайт: обычно у браузеров есть большая база вирусов.*

Если в Интернете пытаются узнать персональные данные, что не нужно сообщать? Укажите правильный вариант ответа.

1. Кличку домашнего питомца.

2. Годовую оценку по математике.

3. *Домашний адрес*.

Можно ли полностью доверять всей информации, размещенной в Интернете? Укажите правильный вариант ответа.

1. Да.
2. *Нет.*

Кому сообщить, если получены угрозы через Интернет? Укажите правильный вариант ответа.

1. Друзьям.
2. *Родителям.*
3. Никому.

Что делать, если при скачивании картинки или мелодии просят отправить СМС? Укажите правильный вариант ответа.

1. Отправить СМС на этот номер.
2. *Поискать прямую ссылку, чтобы скачать без СМС.*

Вы получили письмо от одноклассницы. Она рассказывает о вечеринке, про которую вы в первый раз слышите, и дает ссылку на фотографии. Будете ли вы переходить по ссылке?

1. Да, я перейду, так как вирусы рассылают только с помощью вложенных файлов.
2. Да, я перейду, потому что знаю, от кого письмо.
3. *Нет, я переспрошу у одноклассницы лично, отправляла ли она мне эту ссылку, потому что понятия не имею, о чем речь.*

Злоумышленникам несложно подобрать простой пароль от электронной почты, поэтому «Яндекс.Почта», например, рекомендует создавать сложные пароли. Какой из этих паролей сложный?

1. 23052008 (дата рождения).
2. qweriasbf567 (пароль, в котором больше восьми символов).
3. *Pripevo4k@ (пароль, состоящий из прописных и строчных букв, цифр и символов).*

При загрузке компьютера на экране появляется сообщение: «Ваша операционная система заблокирована. Отправьте СМС на номер XXX и получите код для снятия блокировки». Как поступить?

1. Перезагрузить компьютер, возможно, само пройдет.
2. *Скачать на съемный носитель специальную антивирусную программу, а затем проверить и вылечить с ее помощью компьютер.*

3. Отправить СМС на указанный номер, получить код и снять блокировку.

Одноклассники делают общую фотографию класса. В каком случае фотография будет содержать персональные данные? Укажите один или несколько правильных вариантов ответа.

1. *Если на фотографии указан номер школы, класса и каждый ученик подписан (фамилия, имя).*

2. На фотографии указан номер школы и класса.

3. *На фотографии каждый ученик подписан (фамилия, имя).*

4. Такая фотография не может содержать персональные данные.

5. *Если на фотографии указан номер школы, класса и каждый ученик подписан (только имя).*

По каким признакам можно понять, что компьютер заражен вирусом? Укажите все верные варианты. Укажите один или несколько правильных вариантов ответа.

1. *Вирус может никак не проявлять своего присутствия. Лучше всего просмотреть отчет антивирусной программы.*

2. *Компьютер стал работать медленнее.*

3. *С компьютера отправляются письма, которые вы не отправляли.*

4. *Друзья жалуются, что вы отправляете им спам, хотя вы этого не делаете.*

Как следует вести себя в Интернете? Укажите один или несколько правильных вариантов ответа.

1. *Говорить взрослым, если кто-то в Интернете надоедает тебе.*

2. *Посещать музеи, выставки, картинные галереи, пользуясь ресурсами Интернета.*

3. *Не обмениваться при помощи Интернета фотографиями с незнакомцами.*

4. Рассказывать незнакомым людям информацию о себе и своей семье.

5. *Не открывать электронные сообщения от незнакомых людей и не загружать вложенные в них файлы.*

Надежный пароль состоит из прописных и строчных букв, цифр, знаков препинания. Рекомендуется придумывать разные пароли для сайтов,

почты и социальных сетей. Что НЕ относится к числу самых ненадежных паролей? Укажите правильный вариант ответа.

1. Простые слова.
2. Слова наоборот.
3. Дата рождения.
4. *Последовательность цифр.*
5. Инициалы человека.
6. Кличка питомца.

К чему могли получить доступ злоумышленники, получив логины и пароли от почтовых ящиков? Укажите один или несколько правильных вариантов ответа.

1. *Переписка, в том числе фотографии и конфиденциальная переписка*.
2. *Другие сайты, на которых используются тот же пароль*.
3. *Список контактов (адресатов) пользователя*.
4. Доступ на сайты, где используется двухфакторная аутентификация (подтверждение с помощью СМС).

Приложение 5.

Примерные вопросы для обсуждения на круглом столе «Безопасность в сети Интернет»

Назовите плюсы Интернета. Укажите один или несколько правильных вариантов ответа.

«–» Интернета	**«+» Интернета**
Нецензурные слова в чатах	Возможность общения
Угрозы насилия	Online библиотеки
Агрессивные сетевые игры	Можно посмотреть другие страны, не выходя из дома
Спам	Оперативность получения информации
Возможность кражи персональных данных	Получение дополнительного образования
…	…

Каковы, по вашему мнению, причины интернет-травли?

Чем интернет-травля эмоционально тяжелей обычной?

Как защититься от кибербуллинга?

Как создать себе онлайн-репутацию?

Как поступить в случае интернет-агрессии?

Как реагировать на единичные оскорбительные сообщения?

Что предпринять, если стал свидетелем кибербуллинга?

Как поступить с интернет-агрессором?

Как относиться к агрессивным сообщениям?

Что делать, если оскорбительная информация размещена на сайте?

Приложение 6.

Вопросы для квеста или брейн-ринга

Что следует сделать для предотвращения заражения компьютера вирусами?

Ответ:

1. Установить качественный антивирус.
2. Установить программу «антишпион».
3. Регулярно обновлять сигнатурные базы.
4. Выполнять ежедневное сканирование.
5. Блокировать автоматический запуск.
6. Блокировать просмотр изображений в Outlook.
7. Не переходить по ссылкам в электронной почте и не открывать вложения.
8. Использовать брандмауэр (файрвол).

Какие действия в Интернете преследуются Уголовным Кодексом Российской Федерации?

Ответ:

1. Неправомерный доступ к компьютерной информации.
2. Создание, использование и распространение вирусов.
3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Вам пришло письмо с вложением от неизвестного пользователя. Ваши действия?

Ответ: не открывать письмо.

Чем потенциально опасны социальные сети?

Ответ:

1. Возникновение проблемы нарушения конфиденциальности.
2. Возможное хакерство и взлом паролей.
3. Возможное возникновение виртуальных двойников.
4. Появление интернет-зависимости.
5. Риск попасть в объектив камеры. И др.

Если вирус обнаружен, что следует сделать?

Ответ:

1. Отключить компьютер от Интернета.
2. Загрузить компьютер в безопасном режиме.
3. Проверить наличие на компьютере новейшей версии антивирусных программ.
4. Проверить наличие на сайте производителя установленного антивирусного программного обеспечения информации о специальных утилитах, необходимых для удаления вредоносной программы.
5. Если компьютер подключен к локальной сети, отключить его от сети.
6. Провести полную антивирусную проверку компьютера.
7. Обратиться за помощью в службу техподдержки производителя установленного на компьютере антивирусного программного обеспечения.

Что такое сайт?

Ответ: массив связанных данных, имеющий уникальный адрес и воспринимаемый пользователем как единое целое.

Чем опасны сайты-подделки?

Ответ: могут иметь недостоверную информацию, а также похищать персональные данные пользователя (логины и пароли от социальных сетей, номера кредитных карт).

Что такое спам?

Ответ: массовая рассылка назойливых рекламных писем лицам, не соглашавшимся их получать.

Что относится к спаму?

Ответ:

1. Реклама, в том числе незаконной продукции.
2. Фишинг; Chain Letters, или «цепочечные» письма.
3. Письма религиозного содержания.
4. Письма, содержащие вирусы.
5. Массовая рассылка от имени другого пользователя. И др.

Назовите правила сетевого этикета.

Ответ:

1. Грамотно и удобочитаемо писать сообщения.
2. Избегать транслита или замены букв схожими символами.
3. Не набирать слова целиком прописными или заглавными буквами, не чередовать регистр, не ставить множество знаков препинания и смайлов подряд.
4. Разделять длинный текст на абзацы.
5. Соблюдать языковые нормы.
6. Не использовать не принятый в сообществе сленг и вставлять в текст иностранные слова.
7. Сокращать сообщения.
8. Не игнорировать корректные вопросы других пользователей.
9. Не писать в социальных сетях сообщения для привлечения к себе внимания.
10. Избегать некорректных ответов.
11. Избегать флейма, флуда, спама, оффтопа и др.

Что такое цифровой портрет?

Ответ: все то, что пользователь пишет, выкладывает в Интернет.

С кем не следует общаться в Интернете?

Ответ: с незнакомыми людьми.

Какие сведения не являются персональными данными?

Ответ: только фамилия и инициалы или только адрес проживания.

Что такое вредоносная программа?

Ответ: любое программное обеспечение, используемое для получения несанкционированного доступа к информации или ресурсам компьютера с целью хищения, удаления, искажения или подмены данных.

Назовите методы маскировки вирусов.

Ответ:

1. Невидимые вирусы.
2. Шифрование своего кода.
3. Полиморфные вирусы.
4. Неизменение длины файлов.

Назовите способы мошенничества в Интернете.

Ответ:

1. Интернет-лотереи и конкурсы.
2. Кардинг.
3. Финансовые пирамиды.
4. Фишинг.
5. Блокировка доступа к электронной почте, аккаунтам.
6. Интернет-магазины с предоплатой за товар.

Назовите признаки интернет-зависимости.

Ответ:

1. Постоянный поиск информации в Сети.
2. Пристрастие к виртуальному общению и знакомствам: большие объемы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Сети.
3. Игровая зависимость – навязчивое увлечение сетевыми компьютерными играми.
4. Навязчивая финансовая потребность: игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянное участие в интернет-аукционах.
5. Пристрастие к просмотру фильмов через Интернет.

Что предпринять при получении большого количества спама?

Ответ:

1. Создать адрес электронной почты только для переписки и не использовать его для регистрации на интернет-сайтах.
2. Не отвечать на спам, не открывать вложения и не переходить по ссылкам, содержащимся в спам-сообщениях.
3. Защитное программное обеспечение должно содержать средства защиты от спама.

Как хранить важные файлы?

Ответ:

1. Делать резервные копии.
2. Использовать надежные носители информации (жесткие диски).
3. Хранить данные в облачных сервисах.

Можно ли проникнуть в незащищенный компьютер другого пользователя с другого компьютера?

Ответ: можно.

Какие меры необходимо принять, чтобы нежелательные посетители не могли проникнуть в компьютер через Интернет?

Ответ:

1. Установить антивирусное программное обеспечение.
2. Всегда закрывать обозреватель Интернета после использования.
3. Установить брандмауэр.

Что необходимо при общении в чатах?

Ответ: выяснить правила чата и действовать согласно им.

Какую информацию не следует разглашать в чатах и группах социальных сетей?

Ответ: свои персональные данные и данные родителей, друзей и т.д.

Что сделать при размещении на собственном веб-сайте ссылки на веб-страницу другого пользователя?

Ответ: спросить разрешения другого пользователя.

Вы хотите разместить сделанную вами фотографию друга на своей странице в социальной сети. Как правильно поступить?

Ответ: получить разрешение друга.

Законно ли выдавать себя за другого человека в Интернете?

Ответ: незаконно.

Какую персональную информацию не следует публиковать в сети Интернет в открытом доступе?

Ответ:

1. Номера телефонов.
2. Полный домашний адрес.
3. Место работы или учебы.
4. Дату рождения.
5. Данные документов.

Какими могут быть последствия хакерской атаки для компьютера?

Ответ: нарушение работы программного обеспечения, целостности информации или же ее конфиденциальности.

Поддельный сайт – это…

Ответ: сайт, имитирующий другой сайт, но имеющий отличия от оригинала.

Как распознать поддельный сайт?

Ответ: поддельный сайт имеет схожий с настоящим электронный адрес, схожие цвета, но имеет дефекты, пунктуационные или орфографические ошибки, старые даты новостей, измененный шрифт, нечеткое написание текста. На поддельном сайте отсутствуют контактные данные, также могут публиковаться просьбы отправить СМС с некоторым текстом на номер телефона и т.д.

Каковы ваши действия при получении от друзей неожиданных файлов неизвестного содержания?

Ответ: удалить письмо, не открывая его.

Какое действие предпринять, если в почтовый ящик пришло письмо, в котором говорится, что его надо переслать пяти друзьям?

Ответ: не пересылать письмо.

Что такое кибербуллинг?

Ответ: Кибербуллинг (электронная травля) – это вид преследования, преднамеренные агрессивные действия систематически на протяжении долгого периода времени, осуществляемые лицом или группой лиц с использованием электронных форм взаимодействий, направленных против жертвы, которая не может себя защитить. Это может происходить через СМС-сообщения, социальные сети, создание компрометирующих

веб-страниц или размещение унижающих, оскорбляющих видео, фотоматериалов и др.

Как надо хранить свои пароли (от электронной почты или профиля в социальной сети и т.д.)?

Ответ: использовать менеджер паролей.

Как называется мошенничество, при котором злоумышленники обманом выманивают у доверчивых пользователей сети личную информацию?

Ответ: фишинг.

Как вирус может попасть в компьютер?

Ответ: вирусы попадают на жесткий диск компьютера или его оперативную память через мобильные хранилища данных (гибкие дискеты, диски, флэш-накопители), но больше всего вирусов приходит из Интернета: через электронную почту, мессенджеры, локальные сети.