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

(28–30 октября, по выбору образовательной организации)

Москва

2020

Аннотация

Рекомендации разработаны в целях оказания методической помощи педагогическим работникам начального общего, основного общего, среднего общего образования в организации и проведении «Дня Интернета. Всероссийского урока безопасности школьников в сети Интернет» (28–30 октября, по выбору образовательной организации).

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 общеобразовательной 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 тематических уроков, описание их организационной и содержательной составляющих, возможных форм организации образовательной деятельности обучающихся, дополнительные материалы для учителя, ссылки на тематические ресурсы и рекомендации по их использованию.

Пояснительная записка

Информационная безопасность обучающихся в сети Интернет – актуальный вопрос на протяжении последних лет *(см. Приложение 1).* А с учетом дистанционного обучения (из-за сложной эпидемиологической обстановки, сложившейся в 2020 году) ежедневное использование обучающимися компьютера увеличилось по времени, Интернет стал одной из немногих возможностей для общения со сверстниками и учителями.

Введение электронного обучения и дистанционных образовательных технологий в образовательный процесс привело к необходимости получения обучающимися компетенций по организации самостоятельной работы в сетевом информационном пространстве, включая поиск и освоение рекомендованных цифровых образовательных ресурсов, а также поддержку сетевого взаимодействия как с преподавателем, так и с другими обучающимися в процессе коллективной работы.

Опыт дистанционного обучения показал, что обучающиеся наиболее компетентны в сфере работы с контентом в Сети и наименее компетентны в вопросах современной кибербезопасности. Обучающиеся научились искать информацию и общаться в социальных сетях, но им очень трудно даются критическая оценка найденного, нравственная оценка контента и взаимодействие с интернет-сообществами. Активное использование открытых электронных ресурсов предполагает риски столкновения с информацией, угрожающей психологическому здоровью обучающихся (контентные риски (информация, содержащая сцены насилия, агрессии, эротики и порнографии, ненормативной лексики), кибербуллинг, хищение персональной информации, интернет-зависимость и т.п.) *(см. Приложение 2).*

Информационная безопасность детей и подростков является 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 создания надежного и безопасного Интернета для обучающихся необходимо действовать в разных направлениях: психологических, нравственных, с применением современных прикладных программ; организовать совместную целенаправленную воспитательную работу педагогическим работникам и родителям обучающихся.

Работа с обучающимися должна вестись на каждом уровне образования: начального общего, основного общего и среднего общего образования. На каждом этапе работы необходимы специальные формы и методы обучения в соответствии с возрастными особенностями обучающихся. Формирование навыков информационной безопасности и сетевой компетентности должно осуществляться на уроках по всем учебным предметам и во внеурочной деятельности.

Всероссийский урок безопасности обучающихся в сети Интернет ежегодно включается в формируемый Министерством просвещения Российской Федерации Календарь образовательных событий, приуроченных к государственным и национальным праздникам Российской Федерации, памятным датам и событиям российской истории и культуры. В соответствии с письмом Министерства просвещения от 5 июня 2020 г. № ВБ-1206/04 «О направлении Календаря образовательных событий на 2020/21 учебный год» «День Интернета. Всероссийский урок безопасности школьников в сети Интернет» предлагается провести в общеобразовательных организациях 28–30 октября 2020 года (по выбору образовательной организации).

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

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

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

– Указ Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»;

– национальный проект «Образование» (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам (протокол от 24 декабря 2018 г. № 16), федеральный проект «Цифровая образовательная среда»;

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

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

– приказ Минобрнауки России от 06 октября 2009 г. № 373 «Об утверждении и введении в действие федерального государственного образовательного стандарта начального общего образования» (с изменениями и дополнениями);

– приказ Минобрнауки России от 17 мая 2012 г. № 413 «Об утверждении и введении в действие федерального государственного образовательного стандарта среднего общего образования» (с изменениями и дополнениями);

– приказ Минобрнауки России от 17 декабря 2010 г. № 1897 «Об утверждении федерального государственного образовательного стандарта основного общего образования» (с изменениями и дополнениями);

– Рекомендации парламентских слушаний «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве», прошедших 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» (с изм. и доп.).

Цель методических рекомендаций: оказать методическую помощь педагогам в организации и проведении «Дня Интернета. Всероссийского урока безопасности школьников в сети Интернет».

Задачи методических рекомендаций:

– оказать содействие педагогам в осмыслении актуальности и значимости тематического и содержательного поля проблемы обеспечения безопасного поведения обучающихся в сети Интернет;

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

– предложить педагогам общеобразовательных организаций различные варианты проведения тематического урока с учетом условий и ресурсов общеобразовательной организации;

– предложить педагогам эффективные подходы к методической, содержательной и технологической составляющим тематического урока с учетом возрастных особенностей обучающихся, степени их подготовленности к восприятию материала.

СОДЕРЖАНИЕ МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ

Потенциальные угрозы для обучающихся со стороны открытого сетевого информационного пространства

Риски, с которыми сталкивается пользователь Интернета, многоплановы. Их несет в себе всевозможная информация, размещаемая в сети Интернет самыми разными людьми со столь же разными намерениями. Как отмечают исследователи проблемы, само понятие риска является субъектно-отнесенным: риск связан с ситуацией, в которой возможен неблагополучный исход, с ситуацией опасности, но исход зависит от выбора и действий человека.

В ряду актуальных для сегодняшней интернет-среды рисков, связанных с использованием Сети детьми и подростками, специалисты выделяют следующие:

- ***контентные риски*** – это материалы (тексты, картинки, аудио-, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.;
- ***коммуникационные риски*** связаны с межличностными отношениями интернет-пользователей и включают в себя риск подвергнуться оскорблениям и нападкам со стороны других. К числу таких рисков относятся незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др. Для подобных целей используются различные чаты, онлайн-мессенджеры, социальные сети, сайты знакомств, форумы, блоги и т.д.;
- ***электронные (кибер-) риски*** – это возможность столкнуться с хищением персональной информации, шпионскими программами, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке и т.д.;
- ***потребительские риски*** – злоупотребление в Интернете правами потребителя. Это риск приобретения товара низкого качества, различных подделок, контрафактной и фальсифицированной продукции,

риск потери денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибермошенничества и др.;

- ***интернет-зависимость*** – навязчивое желание войти в Интернет и неспособность вовремя выйти из него, патологическая, непреодолимая тяга к Интернету, оказывающая пагубное воздействие на бытовую, учебную, социальную, семейную или психологическую сферу жизнедеятельности;

- риски, связанные с вовлечением несовершеннолетних в ***опасные группы и сообщества***. Это, прежде всего, так называемые группы смерти, которые побуждают детей и подростков к выполнению опасных заданий, приводящих в конечном итоге к суициду. Это также экстремистские группы, внушающие несовершеннолетним идеи о несправедливости мироустройства и их особом предназначении в «улучшении мира» посредством его «очищения от недостойных» и вовлекающие в незаконную экстремистскую деятельность. Это и группы, предлагающие несовершеннолетним «работу», заключающуюся в незаконной деятельности (прежде всего, в распространении наркотических и других запрещенных веществ и т.п.).

Каждый из этих видов рисков способен принести непоправимый ущерб эмоциональному благополучию и психологическому, а порой и физическому здоровью ребенка.

Задача педагогов в связи с этим состоит в том, чтобы своевременно указать на наличие данных рисков, предостеречь обучающихся от необдуманных поступков в Интернете, сформировать у обучающихся навыки критического отношения к получаемой в Сети информации, воспитать культуру безопасного использования Интернета.

Предлагаем педагогам начального общего, основного общего и среднего общего образования следующую примерную тематику проведения тематических уроков в рамках Дня Интернета (тематика представлена в соответствии с предметными областями).

№ п/п	Предметная область / учебные предметы	Примерная тематическая направленность урока
1.	Математика и информатика (математика, алгебра,	«Безопасная прогулка по интернет-острову», математический квест «Безопасный

	геометрия, информатика)	Интернет», «Математическое интернет-королевство и способы его защиты», «Программные способы защиты сети Интернет», «Спам, вирусы, программы-шпионы и способы борьбы с ними», «Защитный сетевой экран», «Умные алгоритмы сети Интернет», «Что такое криптография и зачем она нужна?», «Кто придумал «Энигму»?» и др.
2.	Русский язык и литература, иностранный язык	«Нецензурная лексика в Интернете: за и против», «Как писать ответ хейтерам и троллям», «Сказка о золотых правилах безопасности в сети Интернет», «Фейки и как не попасться на них», «Лингвистическая безопасность пользователей Рунета», «Превед, медвед! или Нет олбанскому языку», «Американизмы и заимствованные слова в Интернете», «Интернет-письмо Татьяны Онегину» и др.
3.	Естественно-научные предметы (окружающий мир, природоведение, биология, физика, химия, астрономия)	«Интернет-зависимость и как с ней бороться», «Интернет и твое здоровье», «Анонимность в Интернете – миф», «Вирусы компьютерные и биологические», «Каналы утечки компьютерной информации: пьезоакустические, электромагнитные, оптические и другие», «Химическая безопасность и интернет-безопасность: сходство и различия» и

		др.
4.	Общественно-научные предметы, основы духовно-нравственной культуры народов России (история, обществознание, география, основы духовно-нравственной культуры народов России)	«Опасные группы и сообщества: способы противостояния им», «Контрафактная и фальсифицированная продукция в сети Интернет», «Сетевой этикет», «Персональные данные и почему их надо беречь», «Способы противостояния сетевым сектам», «Страны мира с самым безопасным Интернетом»
5.	Тематические мероприятия внеурочной деятельности	*Конкурсы детских работ*: «Любимые сайты нашей семьи», «Мои правила безопасного Интернета». *Классные часы*: «Безопасность в сети Интернет» (5–6-е кл.), «Развлечения и безопасность в Интернете», «Темная сторона Интернета» (7–8-е кл.), «Как обнаружить ложь и остаться правдивым в Интернете», «Остерегайся мошенничества в Интернете» (9–11-е кл.)

Фильтрация и блокировка нежелательного контента

Один из самых простых и действенных способов воспрепятствовать обучающимся получить преднамеренный или случайный доступ к нежелательному контенту – использование программного обеспечения, осуществляющего принудительную фильтрацию и блокировку определенных веб-сайтов и позволяющего пользователям получать доступ только к предварительно одобренным интернет-ресурсам.

Сайтами, содержащими вредоносную информацию для несовершеннолетних лиц, признаются интернет-ресурсы, где допускается изображение сцен физического и психологического насилия и сексуальных действий, присутствует информация, поощряющая наркоманию, курение и

алкоголизм, ведение нездорового образа жизни, суицид, участие в азартных играх и лотереях, половую распущенность, демонстрацию гипноза и паранормальных явлений, а также компьютерные игры, вызывающие агрессивность.

В статье 14 Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» сказано, что «…доступ к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, в местах, доступных для детей, предоставляется… при условии применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию».

Использование специализированного программного обеспечения по фильтрации нежелательного контента и блокировке вредоносных сайтов сети Интернет является одним из обязательных условий применения компьютерных технологий в общеобразовательной организации. Учителя, методисты и вспомогательный персонал могут помочь определить, какие сайты должны быть заблокированы. Помимо этого, в школе целесообразно проводить регулярные аудиты используемых открытых образовательных интернет-ресурсов на предмет оценки их содержания с точки зрения наличия нежелательного контента и определения необходимости их дополнительной фильтрации или блокировки.

Технические средства контентной фильтрации должны быть сконфигурированы и настроены таким образом, чтобы обеспечивать разграничение доступа пользователей к выбору и настройкам режимов работы средств контентной фильтрации и не давать возможности их несанкционированного отключения. В настоящее время общеобразовательным организациям и другим образовательным организациям доступен широкий набор программных средств фильтрации и блокировки вредоносных сайтов.

Учебно-методические материалы
для организации и проведения занятий по обучению
безопасному поведению обучающихся в сети Интернет

Рекомендации педагогам начального общего образования

С обучающимися 1–4-х классов рекомендуется провести беседу, урок-путешествие, урок-викторину, урок-соревнование, урок-сказку, урок-сюрприз, тематический классный час.

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

Большой интерес у обучающихся 1–4-х классов вызывает творческое задание – ***сочинение сказки***. Если у детей не получается сочинить сказку самим, можно предложить им самостоятельно придумать начало, конец или продолжение. Главное требование к сочинению сказки – она должна учить чему-то хорошему («Как Мышонок учился безопасному поведению в сети Интернет», «Сказка о золотых правилах безопасности в сети Интернет» и др.).

Пример сказки

Давным-давно Интернет был чистым. Владел им Великий Добрый Князь. Но однажды Темный Лорд решил забрать себе Интернет. Нанял он себе трех великих бойцов.

Первый боец был искусным мастером. Троян звали его. Представился он программой безобидной и попросил установить. Князь, видя любезность, выполнил требование. Тогда Троян начал творить недобрые дела. Все письма он удалил, файлы нужные уничтожил. Хозяином стал Троян в компьютере Князя.

Вторым стал Спам. Отправил Темный Лорд его Князю. В письме говорилось о том, чтобы Князь переслал его другим. Князь, не подумав, сделал это. Засорил Спам весь Интернет.

Третьим бойцом стал Червь. Попав в компьютер, Червь стал размножаться. Почти остановил он работу операционной системы.

Долго горевал Князь и проклинал Темного Лорда. Но вдруг в княжестве появился Антивирус. Обещал помочь Антивирус Князю и с Трояном, и со Спамом, и даже с Червем. Три дня и три ночи бился

Антивирус с бойцами, но победил. Сверг Антивирус Темного Лорда. И приказал Князь установить Антивирус на все-все компьютеры. И стал Антивирус помогать во всем Князю. Очистили они вместе весь Интернет. И не было теперь вирусов на свете.

Даниил К.

В рамках Всероссийского урока безопасности школьников в сети Интернет в 1–4-х классах целесообразно:

– ознакомить обучающихся с правилами ответственного и безопасного поведения в современной информационной среде, способами защиты от противоправных посягательств в Интернете и мобильной (сотовой) связи;

– формировать критическое отношение обучающихся к информационным сообщениям (СМИ, Интернет, СМС и др.), акцентировать их внимание на способах отличия достоверных сведений от недостоверных, способах избегания вредной и опасной для них информации, приемах распознавания признаков злоупотребления доверчивостью и на том, как сделать более безопасным свое общение в сети Интернет;

– способствовать развитию навыков безопасного общения в социальных сетях (сетевой этикет) – при общении не обижать своих виртуальных друзей, избегать выкладывания в Сеть компрометирующей информации, не позволять себе оскорбительных комментариев и т.д.

Чем опасен Интернет для детей?

Почему об опасности Интернета все чаще говорят психологи, педагоги и родители? Потому что содержание контента в Сети может негативно влиять на психическое состояние ребенка, даже на физическое отставание в развитии. Дети могут так увлечься общением в Интернете и онлайн-играми, что результатом может стать отстранение от реального мира и отставание в развитии, общем и всестороннем.

По данным «Лаборатории Касперского» за 2019 год, чаще всего дети активно используют Интернет для общения – на соцсети и мессенджеры приходится 67% активностей. А так как соцсетями можно пользоваться только с 14 лет, то ребята сознательно приписывают себе лишние года при регистрации аккаунта.

Правила-памятки «Безопасный Интернет для детей»

№ 1

Ни под каким предлогом не раскрывай свои личные данные.

Бывает так, что сайт требует ввода твоего имени. В этом случае следует придумать себе псевдоним (другое имя). Не заполняй строчки, где просят ввести твою личную информацию: адрес, фамилию, дату рождения. Ведь неизвестно, кто может посмотреть эту информацию и потом воспользоваться ей, так как воры и мошенники есть не только в виртуальной, но и в реальной жизни.

№ 2

Старайся посещать те страницы в Интернете, которые советуют тебе родители и педагоги. Они тебя очень любят и никогда плохого не посоветуют! Тебе хочется быть взрослым и самостоятельным, но в этом случае проявлением взрослости как раз и будет то, что ты следуешь советам взрослых.

№ 3

В Сети есть страницы с недетским содержанием, и ты можешь случайно попасть на них. Расскажи об этом родителям, если тебя что-то встревожило или смутило. И помни о том, что многие сторонние ссылки на сайтах ведут на страницы с неприятным содержанием.

№ 4

В Интернете у тебя могут появиться друзья. Если ты захочешь встретиться с интернет-другом в реальной жизни, обязательно сообщи об этом родителям. Не всегда друзья из Интернета такие же дружелюбные и в жизни. И девятилетняя девочка может оказаться тридцатилетним дяденькой, который может тебя обидеть.

№ 5

Никогда без ведома взрослых не отправляй СМС, чтобы получить информацию из Интернета. Часто мошенники заманивают яркими сообщениями типа: «Только сегодня! Уникальный шанс! Участвуй и выигрывай!» Ты щелкаешь на сообщение, где появляется информация: «Для того чтобы принять участие в розыгрыше, тебе необходимо прислать

СМС». Остановись! Ведь одна, казалось бы, безобидная СМС может стоить тебе больших денег.

№ 6

В целом Интернет опасен не более, чем весь окружающий мир. Чтобы обеспечить свою защиту в Интернете, нужно знать об опасностях и способах борьбы с ними. Теперь их ты знаешь, знаешь и правила поведения в Сети. Придерживайся этих правил, и Интернет принесет тебе много полезного.

Не забывай, что Интернет – не главное увлечение в жизни, а всего лишь хранилище разнообразной информации. Кроме Интернета, у тебя должны быть любимые книги, занятия спортом и прогулки с друзьями на свежем воздухе!

Рекомендации педагогам основного общего образования

С обучающимися 5–9-х классов целесообразно провести беседу, урок-дискуссию, урок-практикум, тренинг, урок-консультацию, урок-турнир, классный час.

Особенно привлекательны для подростков активные методы обучения. Для вовлечения обучающихся в познавательно-интеллектуальную деятельность на уроке целесообразно использовать интерактивные материалы, видеоролики.

Большой интерес у обучающихся 5–9-х классов вызывает проектная деятельность, которая стимулирует развитие детской самодеятельности, способствует реализации принципа сотрудничества ребенка и взрослого, позволяет сочетать коллективное и индивидуальное в образовательном процессе с учетом интересов и потребностей обучающихся. Проектная деятельность ориентирована на развитие исследовательской, творческой активности обучающихся, на формирование универсальных учебных действий.

Примерная тематика проектов: «Мои правила безопасного Интернета», «Научим правилам поведения в Интернете младших братьев и сестер», «Безопасность в Сети».

Тематический урок можно построить в форме дискуссии, стимулирующей инициативность, развитие рефлексивного мышления, познавательный интерес обучающихся. В дискуссию на равных правах включаются и обучающиеся, и педагоги. Итогом дискуссионного

обсуждения должна стать формулировка вывода по поставленному вопросу.

Примерные темы дискуссий:

«Интернет и игровая зависимость».

«Как не стать жертвой сети Интернет».

«Как сделать работу в Сети безопасной».

«Зачем нужен безопасный Интернет».

«Какие угрозы существуют в сети Интернет».

«В Интернете есть много интересного, но можно столкнуться и с негативной информацией».

«Мой опыт борьбы с угрозами Интернета».

Примерные вопросы к дискуссии по теме «Интернет: за или против?»:

- ✓ Интернет как информационный источник: плюсы и минусы.
- ✓ Нужно ли вводить ограничения в пользовании Интернетом?
- ✓ Какие меры нужно принимать для того, чтобы человек не стал «рабом» Интернета? Приведите примеры интернет-зависимости.
- ✓ Согласны ли вы с утверждением, что Интернет – это возможность найти интересного собеседника, близкого друга и решить проблему одиночества?
- ✓ Можно ли сегодня обойтись без социальных сетей?
- ✓ Как вы думаете, умеете ли вы совмещать жизнь в гаджетах с реальной жизнью?

По итогам обсуждения заполняется таблица:

ИНТЕРНЕТ	
за	**против**
✓ общение без границ в реальном времени; ✓ возможность оперативного глобального поиска информации; ✓ передача файловой информации без использования внешних носителей; экономия времени при осуществлении онлайн-покупок и банковских	✓ подмена реального общения виртуальным; ✓ вред здоровью; ✓ распространение нелегальной информации; ✓ возможность получения недостоверной информации; ✓ электронный спам; ✓ интернет-мошенничество;

операций; ✓ возможность дистанционного образования; ✓ дополнительные рабочие места и т.д.	✓ вторжение в личную жизнь; ✓ игромания и киберзависимость и др.

В ходе тематического урока рекомендуем подвести обучающихся к выводам, сформулированным ниже.

10 правил разумного использования Интернета

1. Помни: все, что попадает в Интернете, остается там навсегда! Поэтому никогда не выкладывай в открытый доступ свои личные данные: настоящее имя, номер телефона, домашний адрес.
2. Если ты пользуешься компьютером в общественном месте, то корректно заверши работу с сервисами: не оставляй пароли на чужом компьютере и всегда выходи из учетной записи.
3. При получении электронных писем научись использовать фильтры для нежелательной почты и не отвечай на подозрительные сообщения.
4. Внимательно относись к файлам, пришедшим по почте: они могут содержать опасные вирусы. Не загружай программы, музыку или файлы из непроверенных источников.
5. Помни, что файлы и текст из Интернета могут быть защищены законом об авторских правах. Пользуясь чужими материалами, не забывай спрашивать разрешения или указывать автора.
6. Не используй Интернет для хулиганства, распространения слухов или угроз. Не забывай об ответственном и порядочном поведении в Интернете.
7. Азартные игры в Интернете связаны с большим финансовым риском. Знай, что играть в азартные игры в Интернете запрещено законом.
8. С осторожностью относись к знакомствам в Интернете, помни, что за ником и аватаркой может быть любой человек.
9. Сообщи взрослым (учителю или родителям), если кто-то или что-то в Интернете угрожает тебе или доставляет неудобства. Посоветуйся со взрослыми о возможных способах защиты.
10. Расскажи взрослым о предстоящей покупке или продаже чего-либо в Интернете, чтобы не рисковать своими денежными средствами.

Викторина «Что нужно знать о безопасной работе в Интернете?»

1. Бывая в Интернете, Вы часто сталкиваетесь с неприятной информацией, которая «лезет со всех сторон», мешает работать в Интернете. Как избавиться от излишней информации и пользоваться только нужными страницами?

- ✓ Установить антивирусную программу.
- ✓ **Установить на свой браузер фильтр.**
- ✓ Установить новый браузер.

2. Антивирусные программы необходимы:

- ✓ для работы во Всемирной сети;
- ✓ для архивации данных;
- ✓ **для выявления вирусов, лечения зараженных файлов и дисков, предотвращения подозрительных действий.**

3. Что вирус может сделать с компьютером?

- ✓ Вирус не опасен – это просто игрушка.
- ✓ **Вирус может удалять данные, отправлять с компьютера сообщения друзьям в социальных сетях, выключать его.**
- ✓ Вирус может действовать, только если ему дать команду.

4. Для предотвращения заражения компьютера вирусами следует:

- ✓ не пользоваться Интернетом;
- ✓ **устанавливать и обновлять антивирусные программы;**
- ✓ установить пароль.

5. Как создавать пароль для работы в Интернете?

- ✓ Использовать свое настоящее имя и личные данные.
- ✓ Использовать адрес электронной почты.
- ✓ **Использовать сложный пароль (сочетание из букв и цифр).**

6. Чем опасны социальные сети?

- ✓ Личная информация становится доступна мошенникам.
- ✓ Компьютер может быть взломан.
- ✓ **Все вышеперечисленное верно.**

7. Законом в Интернете запрещено:

- ✓ размещать информацию о себе;
- ✓ **размещать информацию о других без их согласия;**
- ✓ копировать информацию для личного пользования.

8. Можно ли выдавать себя за другого человека в Интернете?
- ✓ Конечно.
- ✓ Это разрешено только в особых случаях.
- ✓ **Это противозаконно.**

9. Браузер предупреждает, что сайт, на который Вы хотите перейти, заражен вирусом. Что вы предпримете?
- ✓ Можно спокойно перейти: браузер не антивирус.
- ✓ Браузер может ошибаться.
- ✓ **Нельзя переходить, так как у браузеров есть большая база вирусов.**

10. Ваши друзья говорят, что вы рассылаете им спам-сообщения. Что делать?
- ✓ **Проверить компьютер с помощью антивирусной программы, сменить пароль к аккаунту в социальной сети.**
- ✓ Ничего не делать: такое бывает и потом само проходит.
- ✓ Потребовать доказательства.

При проведении тематического занятия рекомендуем использовать:

– *видеоролики* «10 правил безопасного поведения в Интернете», «Безопасность школьников в сети Интернет», «Защита от вредоносных программ»;

– *видеоуроки* Лиги безопасного Интернета: «Персональные данные»; «Открытые сети»; «Виды мошенничества»; «Виды взлома»; «Анонимность в Сети»; «Умные алгоритмы»; «Социальные сети»; «Фейки и как не попасться на них»; «Профессии будущего»; «Безопасный Интернет».

Рекомендации педагогам среднего общего образования

С обучающимися 10–11-х классов целесообразно провести деловую игру, урок-дискуссию, мозговой штурм «Банк идей», мастер-класс, урок-консультацию, коучинг-сессию, квик-настройку (быстрая психологическая индивидуальная настройка на обучение).

Особенно привлекательны для обучающихся среднего общего образования интерактивные формы обучения, например *деловая игра*. Это метод активного обучения, проводимого по определенным правилам и ориентированного на отработку поведения в заданных ситуациях. Обучающиеся примеряют на себя определенные роли, вступают в непосредственный контакт с одноклассниками и учителем и добиваются поставленных в условиях игры целей.

Примерные темы: «Я выбираю безопасность», «Техника безопасности в Сети», «Интернет-риски», «Что дает вам Интернет?».

Примерные кейсы для деловой игры по теме «Я выбираю безопасность»

В ходе деловой игры обучающимся предлагается в группах обсудить содержание предложенного кейса, выделить поставленные в нем проблемы и предложить их решение. В заключение занятия группы проводят презентацию решения своего кейса.

Кейс 1. Интернет и здоровье

Влияние на психику. Веб-серфинг. Влияние Всемирной сети на человеческую психику четко прослеживается прежде всего в поиске информации. Технологии построены таким образом, чтобы с помощью гиперссылок задерживать пользователя Интернета как можно дольше на сайтах, оттягивая его внимание на хаотичное чтение ненужных сведений, которые отвлекают от насущных задач и целей человека. Такая потребность в получении быстрой, не требующей «пережевывания» информации формирует привычку потреблять ее поверхностно, автоматически, что ведет к информационному засорению.

При этом, когда поток поступления информации затихает, человек чувствует пустоту и стремится снова восполнить образовавшийся ее дефицит. Так возникает вред зависимости от Интернета. Всемирная организация здравоохранения в 2017 году признала феномен интернет-зависимости психическим расстройством, вреду последствий которого подвержен каждый десятый юзер.

Интернет также может с легкостью заменить для человека реальное общение, что активно сказывается на его отношениях с реальным социумом. Существует отдельный феномен СМС-зависимости, в результате которой человек начинает бояться реального общения.

Азартные пользователи также рискуют попасться на удочку вреда игровой зависимости, которая чревата серьезными последствиями, вплоть до случаев суицида в результате проигрыша.

Возможности интернет-сервисов так широки, что затрагивают самые тонкие слабости человеческой натуры, в том числе и страсть к покупкам. Доступность совершать быстрые покупки недорогих товаров, не вставая с дивана, развивает шопоголизм.

Воздействие на нервную систему. Во время активной работы в Сети нервная система обрабатывает колоссальные объемы информации. На сегодняшний день один пользователь Интернета ежедневно пропускает через мозг такое большое количество сведений, что это приносит вред информационного перегруза нервной системы, с последствиями утомляемости, бессонницы, неврозов, апатии, повышенной тревожности.

В наиболее серьезных случаях это может привести к возникновению хронических заболеваний нервной системы, поэтому, проводя время в Интернете, крайне важно его структурировать и периодически давать себе перерывы на расслабляющий отдых.

Ухудшение зрения. Проводя долгое время перед экраном гаджета, человек напрягает свое зрение в несколько раз сильнее, и дело здесь не только в мелком тексте перед глазами. Человеческий глаз по своим свойствам имеет сходство с фотоаппаратом. Для того чтобы сделать четкий кадр, состоящий из мерцающих мелких точек, ему необходимо постоянно менять фокус, что увеличивает расход главного пигмента зрения – родопсина, приводящий к близорукости и другим заболеваниям глаз.

У художников близорукость возникает крайне редко, поскольку они все время переводят взгляд с холста на отдаленные предметы, что приносит пользу профилактике нарушений зрения.

Это можно перенять и в работе с гаджетами. Самым простым упражнением будет смена фокуса зрения с ближнего на дальний объект – это станет полезной профилактикой вреда близорукости.

Людям, проводящим много времени в Интернете, специалисты рекомендуют приобрести полезные «компьютерные очки», в которые встроены специальные фильтры, приближающие цветовые параметры экрана к спектральной чувствительности глаза.

Влияние на опорно-двигательный аппарат. Постоянное пребывание в Интернете в статичной позе перед компьютером влечет вред для обменных процессов в организме. Межпозвоночные диски теряют естественные свойства подвижности и больше подвержены деформации, что приводит к быстрому развитию остеохондроза или межпозвоночной грыжи.

Длительная работа за ПК может также привести к нарушению передачи нервного импульса от кончиков пальцев до головного мозга из-за нарушений свойства чувствительности нервных окончаний и возникновению постоянных судорог мышц кистей рук и предплечья.

Сильное перенапряжение сухожильно-связочного аппарата, мышц кистей рук и предплечья ведет к вреду развития туннельного синдрома – защемление нерва в канале запястья может потребовать даже хирургического вмешательства.

Источник: Д. Айвазян. Польза и вред Интернета. Влияние Интернета на наших детей

Кейс 2. Сетевая безопасность. Мошенничество в Интернете

«Узнай местоположение по номеру телефона». Предлагается зарегистрировать программу распознавания либо бесплатно, либо со взносом определенной суммы; программа часто оказывается обыкновенным вирусом. В любом случае человек что-то

теряет – деньги со своего счета или же информацию со своих аккаунтов, связанных с компьютером или телефоном. Либо незадачливого «шпиона» начинают терроризировать звонками и электронными письмами.

«Магазин на диване». Предлагается приобрести желаемый товар по привлекательной цене (раз в пять ниже среднестатистической), а возможно, и вовсе бесплатно – вроде конфискат, вам делают подарок. Единственным условием может оказаться стопроцентная предоплата и оплата доставки. С учетом тарификации цена оказывается той же, что и в любом магазине. Зачастую ждать такую посылку приходится очень долго. При этом существует вероятность, что товар доставлен не будет.

«Лотерея». Вам приходит письмо о крупном выигрыше: вы выиграли деньги / машину / что-то еще, приз будет выслан / счет активирован, как только вы переведете некоторую сумму (пошлина, транспортные расходы и т.д.). Вы не участвовали в конкурсе – неважно. Даже не слышали о нем – тем более. Это очень интересно, просыпается азарт – получить нечто, при этом ничего не делая.

«Отправка СМС». «Ваш аккаунт блокирован, подтвердите СМС… Вы выиграли, отправьте СМС…» Итог: 1 СМС = от 200 до 1000 р.

«Попрошайничество». На почту поступает письмо с просьбой о материальной помощи, так как автор письма – студент / начинающий / в сложной ситуации / денег нет, кушать нечего. На вас никто не давит, желаемая сумма может не указываться. Или в письме указывается довольно нелепая, фантастичная история о человеческих проблемах (с правосудием, с преступниками, с армией, с родственниками – шантаж, угрозы, насилие; возможно давление на жалость) с большим количеством подробностей.

«Техподдержка». Приходит письмо с уведомлением, что аккаунт на каком-либо сайте взломан или может быть заблокирован или удален (и т.д.). Чтобы этого не случилось, необходима оплата. Или: проведение верификации пользователей в связи с мошенничеством, необходимо ввести пароль и кликнуть по ссылке (либо ваша страница взломана – введите пароль).

«Шантаж». К этой категории относятся все сообщения насчет «нелегального доступа к услугам сайта», спама с вашей страницы, угроз выложить в Сеть какие-либо материалы, где главным условием избавления от проблемы являются ваши действия по отправлению денежных средств шантажисту.

Источник: Золотарева Т.Л. Программа занятий по теме «Безопасный Интернет»

Кейс 3. Сетевой этикет

Необходимость обязательного подтверждения полученных сообщений. Электронная почта сегодня заменила телефон. К сожалению, часто корреспонденты (по разным причинам) не подтверждают получение письма.

Итак, вы отправили электронное письмо и очень волнуетесь, дошло ли оно до адресата. И в следующий раз ради собственного спокойствия вы уже отправляете письмо с уведомлением о получении. Но по правилам сетевого этикета такая отметка является признаком неуважения и недоверия к своему партнеру. Лучше после отправки своего сообщения по электронной почте позвонить адресату и уточнить, дошло ли ваше

письмо. Довольно часто для подтверждения используется следующее: после текста основного письма перед вашей подписью пишется фраза «Получение письма просим подтвердить ответным письмом или по указанным ниже телефонам».

По правилам сетевого этикета на электронные письма обязательно нужно отвечать. А время ответа на e-mail не должно превышать двух суток. Если вам необходимо более длительное время для ответа на письмо, стоит объяснить причины задержки.

И обязательно нужно отвечать на письма, содержащие прикрепленные файлы: вы должны подтвердить, что вложение дошло и нормально открылось.

Имейте в виду, что если вы не отвечаете на электронное письмо в течение 7 дней – это явный отказ от общения. Поэтому при желании сохранить деловые отношения вам нужно обязательно через 2–3 дня после отправки электронного письма позвонить или направить повторное письмо своему деловому партнеру для уточнения: дошла до него информация или нет.

Корреспонденту, получившему электронное письмо, достаточно написать два слова: «Спасибо. Получил».

Некоторые сервисы направляют электронное подтверждение того, что отправленное письмо доставлено адресату и им открыто.

Но, во-первых, это не гарантирует стопроцентно, что письмо открыто и прочитано именно тем, кому оно адресовано, а не почтовым роботом. Во-вторых, современные спам-фильтры зачастую блокируют и не пропускают такие автоматические подтверждения.

Недопустимость рассылки без предупреждения файлов большого объема. Даже если вы решили сделать своим коллегам приятное и поздравить их, например, с Новым годом, рассылая сразу по нескольким адресам или индивидуально файлы объемом 2–5 мегабайт, это также считается грубым нарушением сетевого этикета.

Более корректно в этом случае разместить такой большой файл на своей страничке в Интернете, а по электронной почте направить коллегам ссылку на этот сайт. Интернет будет вам благодарен.

Стиль общения. При переписке через электронную почту можно опускать обращения и приветствия и сразу переходить к делу. Но если вы хотите, чтобы ваше электронное письмо носило более официальный характер, рекомендуется использовать следующую формулу обращения: «Добрый день, уважаемый (уважаемая) + имя, отчество адресата». Только после этого следует переходить к цели вашего обращения.

При всей неформальности общения необходимо помнить и выполнять одно из главных правил при составлении электронных писем – соблюдение принципов грамотности и логичности. Тот факт, что электронная почта – быстрый способ связи, вовсе не означает, что она должна быть небрежной. С появлением компьютеров правила русского языка никто не отменял, и читать неграмотный текст с экрана так же неприятно, как и на бумаге.

Обязательно начинайте предложение с прописной буквы и ставьте точки. Имена и названия должны начинаться с прописных букв. Текст, написанный одними строчными без точек и других знаков препинания, трудно читать. Текст же, написанный одними прописными, вообще воспринимается при чтении как

НЕПРЕРЫВНЫЙ КРИК. Поэтому не нужно злоупотреблять этим средством выделения своих сообщений.

Необходимо использовать пропуски (пустые строки) или многоточие для отделения одной мысли от другой, так как в электронном письме они, как правило, играют роль абзаца.

Оформление электронного письма. Во многих организациях существует единый корпоративный стандарт оформления электронных писем, включающий в себя структуру самого письма, правила обращения к клиенту, реквизиты подписи (Ф.И.О., должность, рабочие телефоны, адрес электронной почты и ссылку на сайт организации).

В общем виде структуру делового электронного письма можно представить в следующем виде:

1. «Шапка» в корпоративном стиле.
2. Приветствие.
3. Содержание, цель обращения.
4. Прощание.
5. Личная подпись с указанием контактов.
6. Ссылка на сайт организации.
7. Логотип, если это необходимо.

При оформления электронного письма в обязательном порядке должны быть заполнены поля:

Почтовый адрес получателя (поле «Кому»).

Тема письма (поле «Тема»).

Важность письма, при необходимости.

Текст письма.

Поле «Тема» обязательно для заполнения, иначе ваше письмо может быть удалено как спам. Здесь следует вписать несколько слов, характеризующих тему сообщения.

В некоторых почтовых программах можно указать степень важности сообщения. Это просто необходимо, если адресат получает ежедневно большое количество писем. С пометкой «Важное» письмо получает приоритет при проверке почты. Но злоупотреблять этой функцией не стоит. Важное постепенно потеряет это качество.

Размер электронного письма. Правилами сетевого этикета размер электронного письма определяется следующим образом: электронное письмо должно быть в два раза короче, чем написанное на бумаге. Если вам необходимо переслать важную информацию, содержащую большой объем, то лучше составить краткий сопроводительный текст в электронном письме, а саму информацию оформить в виде вложения (прикрепленного файла).

Если в вашем сообщении есть проблема с объемом и количеством вложенных файлов, то большие файлы разбейте на несколько меньших и разошлите их отдельными письмами. Для запаковки файлов можно использовать популярные программы-архиваторы.

Готовя пересылку большого вложения, превышающую 200–500 килобайт, обязательно предупредите об этом своего респондента.

Адресная книга. При традиционной переписке приходилось либо хранить конверты с адресами, либо записывать их. Помнить электронные адреса всех ваших друзей и партнеров тоже невозможно, да и не нужно. Для этого в любой почтовой программе есть функция «Адресная книга», в которой можно хранить e-mail своих корреспондентов и другую контактную информацию. При использовании этой функции отправить электронное письмо намного проще бумажного, достаточно выделить нужное имя в адресной книге и нажать кнопку «Написать письмо».

Когда электронное письмо придет от респондента, занесенного в вашу адресную книгу, вы всегда будете знать, от кого именно получили электронное сообщение, так как зафиксированный контакт отразится в поле «От».

Смайлики (Smileys). При обычном общении на собеседников не только и не столько воздействуют слова, сколько голос, интонации, мимика, жесты. В этом минус общения через электронную почту: она лишает возможности обмениваться эмоциями. И все же удалось частично преодолеть этот недостаток. В настоящее время в виртуальном общении, в том числе и через электронную почту, широко используются так называемые смайлики (графическое изображение ваших чувств) – рожицы, составленные из точек, запятых, дефисов и других символов. Они способны хоть как-то эмоционально окрашивать тексты. Использование смайликов делает переписку более живой: автор передает не только свои мысли, но и чувства.

Не стоит использовать смайлики при составлении делового письма, в противном случае вы можете приобрести репутацию несерьезного человека.

Источник: Столярова Е.Г. Нетикет – сетевой этикет

Вторым вариантом проведения деловой игры для обучающихся 10–11-х классов может стать ***знакомство с профессиями соответствующей тематики, представленными на образовательном интернет-портале «ПроеКТОриЯ»*** (***https://proektoria.online/***).

Рекомендуется организовать групповую работу обучающихся. Каждая группа, ознакомившись с материалами сайта, представляет профессию по плану: характеристика профессии, основные компетенции специалиста, отрасли, в которых можно построить карьеру.

Примеры профессий

Специалист по информационной безопасности. Человек IT-индустрии. Разрабатывает и внедряет программы, которые противостоят утечкам данных. Осведомлен в работе утилитов Air, Wi-Fi, Bluetooth и GSM, идентификации пользователя по отпечатку пальца или по сетчатке глаза. Создает комплексы безопасности, обучает информационной безопасности других сотрудников.

Сегодня виртуальный мир во многом выигрывает у реального: здесь все проще, быстрее, выгоднее. И чем больше люди в него погружаются,

тем больше работы у программистов, системных администраторов, тестировщиков и других IT-специалистов. Специалист по информационной безопасности защищает все, что они создают.

Специалист по кибербезопасности. Задача – защищать цифровые данные и не допускать их потерю или кражу. Цифровые данные – это все, что существует в электронном виде и может обрабатываться автоматически. Это пароли от аккаунтов в соцсетях, переписки по электронной почте или в мессенджере, документы на флешке, музыка на диске, фрагменты блокбастера, который до конца еще не смонтировали, настройки для дистанционного управления промышленными станками или роботами.

Взломы не единственная беда. Вирус или «червяк» может «уронить» серверы и прекратить работу больниц, заводов, банков, финансовых бирж и даже целого государства. В 2017 году один такой «червь» проник в 520 тысяч компьютеров более чем в 200 странах мира. Программа блокировала работу компьютера и вымогала 300 долларов США. Если выкуп не поступал, то через семь дней она уничтожала все пораженные файлы. Автомобильной компании «Рено» пришлось полностью остановить свои заводы.

Чтобы не допустить виртуальной эпидемии, специалист по кибербезопасности должен знать уязвимые места операционной системы компьютера и языки шифрования, понимать и разбираться, как вирусы попадают в систему.

Специалисты по кибербезопасности работают в крупных финансовых и IT-компаниях, в государственных органах и оборонных ведомствах, где обеспечивают защиту национальной безопасности.

Консультант по безопасности личного профиля. Обычно такого специалиста нанимают люди, чья репутация может пострадать из-за какого-то факта в Интернете. Одно фото в Сети или парочка скандальных комментариев, о которых клиент уже и не помнит, могут стоить ему карьеры и даже обернуться уголовным делом. Задача специалиста – сделать так, чтобы любой, кто ищет информацию об этом человеке, нашел только позитив. Часто бывает, что конкуренты по бизнесу размещают заказные статьи, чтобы перетянуть к себе клиентов. Чтобы хорошо делать свою работу, консультанту нужно разбираться в программировании, быть аналитиком, имиджмейкером, знать юридические тонкости в сфере IT.

Каждый человек, пользуясь Интернетом, оставляет следы. Консультант анализирует профили в социальных сетях и уровень

конфиденциальности заказчиков. Имеет значение, кого человек добавляет в друзья, насколько надежны его пароли и кодовые слова, ведет ли клиент деловую переписку в личных сообщениях, как часто публикует фото, по которым можно вычислить его распорядок дня, место работы или домашний адрес. Важно и то, пользуется ли человек публичными Wi-Fi-сетями, ведь это дополнительный риск утечки паролей и возможной хакерской атаки.

По прогнозам IT-специалистов, уже в ближайшие несколько лет появятся программы точного распознавания пользователей в Интернете, которые позволят отслеживать каждый шаг в Сети. Когда это произойдет, данная профессия станет еще более востребованной.

В заключение занятия рекомендуем обучающимся составить 10 правил – ***законов поведения, предотвращающих возникновение интернет-зависимости***. Все правила фиксируются на доске или ватмане.

Например:

1. Расставить приоритеты.
2. Составить список занятий, которым мешает интернет-зависимость.
3. Планирование – максимально загрузить время делами, которые не связаны с Интернетом или гаджетами.
4. Поставить перед собой цель проводить в Интернете не более определенного количества времени.
5. Следить за тем, сколько времени вы проводите онлайн.
6. Избегать приложений, сайтов и привычек, которые вы считаете проблемными.
7. Выбор замены Интернету. Замена должна быть яркой, положительной, веселой настолько, чтобы всегда было желание отказаться от интернет-серфинга в ее пользу. Это может быть прослушивание любимой музыки, занятие спортом, рисование, ведение личного дневника или беседа с родными или близкими людьми.
8. Заменить виртуальное общение реальным.
9. Придумать себе стимул – награду за привычку проводить ограниченное время у компьютера.
10. Попробовать составить список дел, которыми можно заняться, сократив время пребывания за компьютером: выучить новый язык, путешествовать, посещать галереи и театры, записаться в спортивную секцию и т.п.

Список литературы

1. Бабаш А.В., Баранова Е.К. Информационная безопасность и защита информации: учеб. пособие. – М.: РИОР, 2018.
2. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК-Пресс, 2017.
3. Информационная безопасность. Правила безопасного Интернета. 2–4 классы: учеб. пособие. – М.: Бином. Лаборатория знаний, 2020.
4. Каменских Н., Кострова М. Интернет. Доступ разрешен. – М.: ИД «Комсомольская правда», 2018.
5. Клименко И.С. Информационная безопасность и защита информации. Модели и методы управления. – М.: ИНФРА-М, 2020.
6. Колисниченко Д.Н. Секреты безопасности и анонимности в Интернете. – СПб.: BHV, 2020.
7. Мурсалиева Г. Дети в Сети. Шлем безопасности ребенку в Интернете. – М.: АСТ, 2017.
8. Полезный и безопасный Интернет. Правила безопасного использования Интернета для детей младшего школьного возраста: практ. пособие / под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2017.
9. Полищук Ю.В., Боровский А.С. Базы данных и их безопасность: учеб. пособие. – М.: ИНФРА-М, 2020.
10. Шаньгин В.Ф. Информационная безопасность и защита информации. – М.: ДМК-Пресс, 2017.

Интернет-ресурсы

1. Безопасный Интернет детям от МВД России: https://мвд.рф/Internet_for_kids.
2. «Дети России онлайн»: http://detionline.com/.
3. Лига безопасного Интернета: https://вбезопасныйинтернет.рф.
4. Линия помощи «Дети Онлайн». Бесплатная всероссийская служба телефонного и онлайн-консультирования для детей и взрослых по проблемам безопасного использования Интернета и мобильной связи: http://detionline.com/helpline/about/.
5. «Единый урок. Онлайн-викторины и курсы»: http://единыйурок.дети/.
6. Справочник по детской безопасности в Интернете. Рекомендации по информационной безопасности для всей семьи: http://google.ru/goodtoknow/familysafety/.

7. «Урок цифры»: https://xn--h1adlhdnlo2c.xn--p1ai/.
8. Уроки безопасности в Интернете на сайте «Российской электронной школы»: https://resh.edu.ru/.
9. «Учеба.ру». 15 правил безопасного поведения в Интернете: https://www.ucheba.ru/project/websafety?form=ucheba.spa.
10. «РОЦИТ – ваш помощник в Интернете». Видеоролики для детей об основных угрозах Интернета и о том, как их избежать. Страница сайта Региональной общественной организации «Центр Интернет-технологий» (РОЦИТ), объединяющей активных интернет-пользователей России: https://rocit.ru/video.
11. Защита детей. Ответы на вопросы о детской безопасности в Сети: настройки безопасности, антивирусы, полезные приложения, советы школьникам и родителям: https://kids.kaspersky.ru/.
12. «Персональные данные». На сайте можно узнать о том, что такое «персональные данные», почему в Интернете их надо оберегать и как это сделать, как защитить свой гаджет от вредоносных программ и как общаться в Сети. Здесь же можно пройти тесты на знание правил безопасности в Интернете и поиграть в игры, тренирующие внимание и память: http://xn--80aalcbc2bocdadlpp9nfk.xn--d1acj3b/.
13. «Разбираем Интернет». Все о том, как грамотно пользоваться возможностями Интернета: простые советы, обучающие игры и видеоролики для начинающих пользователей, онлайн-тесты для проверки собственных знаний по интернет-безопасности: http://www.razbiraeminternet.ru/.

ПРИЛОЖЕНИЯ

Приложение 1

История «Единого урока безопасности в сети Интернет»

14 марта 2014 года в Совете Федерации прошли парламентские слушания на тему «Актуальные вопросы обеспечения информационной безопасности детей при использовании ресурсов сети Интернет», на которых спикер Совета Федерации В.И. Матвиенко выдвинула инициативу о проведении ежегодно в учреждениях страны Единого урока по безопасности в сети Интернет.

«Убеждена, что немалую пользу мог бы принести и Всероссийский урок безопасного Интернета, например, в День знаний или Международный день распространения грамотности. И вообще, уроки безопасного Интернета можно было бы включить в школьный курс основ безопасности жизнедеятельности», – подчеркнула спикер Совета Федерации.

Инициатива должна была стать инструментом повышения уровня информационной грамотности миллионов детей в масштабах всей страны и была поддержана Министерством образования и науки России и всеми участниками слушаний, среди которых были представители регионов, школ и общественности.

30 октября 2014 года прошел первый Единый урок безопасности, который охватил более 11 миллионов подростков. Для детей по всей стране были проведены уроки, презентации, круглые столы, квест «Сетевичок» и многие другие мероприятия.

В 2015 году Минобрнауки России включило проведение Единого урока в ежегодно формируемый министерством календарь образовательных событий на учебный год, а программа самого Единого урока была расширена. Так были запущены:

– сетевая площадка для педагогов, на которой размещались полезные материалы для проведения уроков;

– всероссийское дистанционное исследование, которое было направлено на определение сфер жизнедеятельности российских детей в Интернете;

– конкурс детских сайтов «Премия Сетевичок», в ходе которого лучшие детские ресурсы выбирали сами дети в режиме «народного

голосования». Итогом данной работы стало повышение количества вовлеченных несовершеннолетних – в 2015 году участниками Единого урока стало более 13 миллионов детей, а квест «Сетевичок» охватил более 170 000 детей и стал крупнейшим детским проектом в Рунете.

В 2016 году Совет Федерации при проведении Единого урока сфокусировался на привлечении отраслевых специалистов в школы для проведения Единого урока, а также на повышении информационной грамотности педагогов. Так в школы пришли представители МВД, Генеральной прокуратуры, ФНС, органов власти в сфере IT-технологий и представители бизнеса, а также была проведена дистанционная конференция по формированию детского информационного пространства. Проект «Сетевичок», в мероприятиях которого приняли участие более 270 000 детей и более 60 000 педагогов, был выдвинут Минкомсвязью России на престижную премию ООН на Всемирной встрече на высшем уровне по вопросам информационного общества (ВВУИО) и стал полуфиналистом премии.

В 2017 году в Едином уроке приняли участие обучающиеся 32 800 школ, 2 100 000 родителей и 440 000 учителей. В программу урока вошли дистанционные мероприятия для родителей, были разработаны новые материалы для проведения уроков и запущен сайт Единого урока для детей – «Единыйурок.дети».

В начале 2018 года Единый урок по безопасности в сети Интернет стал полуфиналистом конкурса на соискание Премии Всемирной встречи на высшем уровне по вопросам информационного общества, организаторами которой выступают различные организации ООН. Выдвижение Единого урока на конкурс было поддержано Минкомсвязью России, Минобрнауки России, Роскомнадзором и 64 администрациями субъектов Российской Федерации.

В 2019 году программа Единого урока была расширена новыми направлениями и мероприятиями, что нашло свое отражение в плане мероприятий по реализации Концепции информационной безопасности детей на 2018–2020 годы, утвержденном приказом Минкомсвязи России от 27 февраля 2018 г. № 88 (с изменениями, внесенными приказом Минкомсвязи России от 29 июля 2018 г. № 330).

Приложение 2

Словарь основных понятий

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.

Груминг – сексуальное соблазнение ребенка в Сети взрослым мужчиной или женщиной для дальнейшей сексуальной эксплуатации ребенка.

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, здесь высок риск вторжения или мошенничества. Это могут быть 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 (личные) данные – сведения, относящиеся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), которые предоставляются другому физическому или юридическому лицу либо лицам.

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

Секстинг – это отправка интимных фотографий, видео и текстовых сообщений через Интернет.

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

Троллинг – прямое или замаскированное оскорбление участников интернет-сообщества с целью получения негативной реакции или выхода на прямой конфликт с оппонентом.

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.

Флейминг – разжигание спора, публичные оскорбления и эмоциональный обмен репликами в Интернете между участниками в равных позициях.

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.

Хейтинг – негативные комментарии и личные сообщения, иррациональная критика в адрес конкретного человека или явления, часто без обоснования своей позиции.

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.