ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ДОНЕЦКИЙ РЕСПУБЛИКАНСКИЙ ИНСТИТУТ ДОПОЛНИТЕЛЬНОГО ПЕДАГОГИЧЕСКОГО ОБРАЗОВАНИЯ»

Информационно-методические материалы для педагогов образовательных организаций для проведения Республиканского урока безопасности в сети Интернет

Интернет – как океан, есть полезное, есть опасное, можно плыть, а можно утонуть.
М. Докукин

Согласно **Календарю образовательных событий, приуроченных к государственным праздникам, памятным датам и событиям Донецкой Народной Республики**, на 2017/2018 учебный год (письмо Министерства образования и науки Донецкой Народной Республики от 03 августа 2017 г. № 3361/21-21), с целью реализации Концепции развития непрерывного воспитания детей и учащейся молодёжи Донецкой Народной Республики, утверждённой приказом Министерства образования и науки Донецкой Народной Республики от 16 августа 2017 г. № 832, **30 октября 2017 г.** в образовательных организациях Донецкой Народной Республики состоится **Республиканский урок безопасности в сети Интернет.**

По данным, изложенным в докладе ООН Global Broadband Progress от 18 сентября 2017 г., количество пользователей Интернета в мире составляет 3,58 миллиарда человек (общее население планеты – 7,6 млрд). В период с 2000 по 2015 год удельный вес пользователей Интернета увеличился почти в семь раз – с 6,5 до 43 процентов мирового населения. В возрастной группе 16-24 года регулярно используют Интернет 94 % европейцев, в возрастной группе 55-74 лет таких пользователей 46 %.

Такое расширение интернет-аудитории определяет необходимость проведения системной работы в образовательных организациях с обучающимися различных возрастных категорий по формированию их информационной культуры. Стержневым образовательно-воспитательным мероприятием данной системы должен стать **Республиканский урок безопасности в сети Интернет.**

Цель урока: повысить уровень цифровой грамотности и кибербезопасности молодого поколения; обеспечить внимание родителей и педагогов к проблеме детской безопасности в сети Интернет.

Рекомендуем классным руководителям привлечь к организации и проведению урока педагога-психолога образовательной организации, учителей

информатики и ИКТ, педагогов дополнительного образования, реализующих программы научно-технической направленности, заинтересованных родителей и выстроить урок, основываясь на одной из предложенных **содержательных линий**:

- Общение в сети Интернет: компьютерная этика, правила безопасности, возможные риски.
- Интернет-зависимость: симптомы, лечение, профилактика.
- Кибербезопасность: обеспечение конфиденциальности, целостности и доступности данных.
- Защита детей и подростков от нежелательного контента.

При необходимости можно комбинировать указанные содержательные линии, исходя из личностных особенностей обучающихся, информационных запросов детского или подросткового коллектива, для которого будет проводиться урок, а также из возможностей педагогического коллектива образовательной организации, её материально-технической базы.

Перед проведением урока рекомендуем провести анонимный опрос (можно интернет-опрос с использованием Google-формы, Web-анкеты, возможностей социальных сетей) для обучающихся и родителей с целью выявления проблем, связанных с темой урока, чтобы обсудить их и найти возможные пути решения на занятиях с обучающимися и их родителями (возможно, и совместных).

Общение в сети Интернет: компьютерная этика, правила безопасности, возможные риски

(для обучающихся младшего школьного возраста)

> Интернет, он не сближает. Это скопление одиночества. Мы вроде вместе, но каждый один. Иллюзия общения, иллюзия дружбы, иллюзия жизни…
>
> Я. Л. Вишневский

Интернет предоставляет массу удобных сервисов для общения. Теперь не проблема связаться с друзьями, живущими на другом континенте, или передать видеопривет родителям на дачу посреди леса. Форумы, чаты, сервисы обмена мгновенными сообщениями, видеозвонки – бессчётное количество специальных программ готовы прийти на помощь и соединить вас с человеком в любой точке мира.

Попав в Интернет, мы, как правило, первым делом осваиваем социальные сети и мессенджеры: сначала для общения с родственниками и друзьями, а

вскоре и для заведения новых знакомств. В онлайн-общении нет ничего плохого, если подходить к новым друзьям с определённой долей осторожности. Поэтому обязательно нужно помнить правила безопасности при виртуальных знакомствах:

1. Человек в Интернете может представиться кем угодно, но это не значит, что он таким и есть. Если с вами общается, к примеру, голливудский актёр или великий футболист, скорее всего, вас обманывают.

2. Общаясь с незнакомцами, не будьте слишком открытыми. Искренность хороша лишь с близкими друзьями. Не рассказывайте, где и в каких условиях вы живёте, в какую школу ходите, каков ваш распорядок дня. Не рассказывайте ничего такого, чего потом можете стесняться или о чём вы бы не хотели, чтобы узнали все.

3. Насторожитесь, если новый знакомый задаёт вопросы с финансовым подтекстом: сколько стоит ваш автомобиль? Где работают родители? В какие магазины ходите? Когда папа приносит зарплату? Никогда не отвечайте на такие вопросы и не рассказывайте никому подробности вашего семейного бюджета.

4. Если новый знакомый сразу после знакомства предлагает прислать вам какой-то файл (игру, книгу, интересный видеоролик), не принимайте его и ни в коем случае не открывайте. Возможно, таким образом вам хотят подбросить компьютерный вирус.

5. Также с осторожностью относитесь к ссылкам, присланным незнакомцами. Не переходите на другие сайты, если не уверены точно, что знаете, куда они вас приглашают.

6. Если виртуальный знакомый предлагает вам встречу, обязательно сообщите об этом родителям. Пусть они проводят вас и заодно тоже познакомятся с вашим новым другом.

7. Есть темы, о которых никогда нельзя разговаривать с незнакомыми людьми. Одна из таких тем – секс. Если с вами будут заводить беседу на подобные темы, не отвечайте и сразу сообщите родителям.

8. Не принимайте на веру всё, что пишут незнакомые вам люди. Даже если они напишут, что ваша мама сидит у них в гостях и просит вас прийти, не верьте и для начала сами перезвоните маме или папе. Что бы вам ни рассказывали, если информация вас задевает, удивляет или предполагает какие-то действия с вашей стороны, сначала перепроверьте.

9. Если незнакомый человек просит вас прислать свою фотографию или фотографию своего дома, комнаты, родительской машины, в общем, чего-то личного, что касается только вас и вашей семьи, не присылайте ничего.

10. Не рассказывайте незнакомцам о своих планах на будущее – о ближайших поездках, покупках, мероприятиях.

11. Не пересылайте важную информацию (например, логин и пароль) по незащищённым каналам: в чате или на форуме. Хакеры действительно способны перехватить любые данные, отправляемые по незащищённому соединению.

12. Не открывайте доступ к своим постам и фотографиям в социальных сетях для всех – вы не знаете, кто может посетить вашу страницу. Скорее всего, вам не нужно сообщать абсолютно всем пользователям Интернета о каждом своём действии. Установите настройки доступа к странице «Только для друзей».

13. Не подтверждайте каждый запрос на добавление в друзья. Лучше собрать узкий круг настоящих друзей, которых вы знаете и с которыми вам нравится общаться, чем окружить себя толпой незнакомцев. Некоторые из них могут быть действительно опасны.

14. Если общение с новым человеком вам неприятно, но вы не можете его прекратить, сообщите родителям и попросите о помощи. Иногда без вмешательства взрослых просто не справиться.

Со стороны родителей также важно не пускать дело на самотёк и всё же периодически контролировать, с кем и о чём общается их ребёнок. Самый удобный способ (помимо беседы с ребёнком, конечно) – это стать его другом в социальных сетях и отслеживать активности в форумах, группах и т. д. Также отлично помогают программы родительского контроля.

Рекомендуем рассмотреть эти и другие правила компьютерной этики и компьютерной безопасности с обучающимися младшего школьного возраста в **форме**:

- *ролевой игры* «Давайте початимся», «Если тебе написали в соцсети…», «Обменяемся контактами», «Расскажи о своих виртуальных друзьях», «Что можно узнать друг о друге в соцсетях?»; «Что можно и что нельзя размещать на страничке в соцсети?»;
- *анализа ситуаций* «Что ты будешь делать, если…» (ситуации можно предложить, продемонстрировав видео, или, если позволяет материально-техническая база школы, разыграть различные сценарии общения с неизвестными в сети, открыв страничку педагога в социальной сети и общаясь с удалённым помощником по заранее оговорённому сценарию урока – можно задействовать родителей);
- *викторины* «Интернет: можно и нельзя», «Как поступить правильно?»;
- *оформления информационных уголков, памяток, съёмок тематических видеороликов с последующим размещением на страничке класса, образовательной организации в социальной сети;*
- *тематических театрализованных постановок* и т. д.

Интернет-зависимость: симптомы, лечение, профилактика

(для обучающихся среднего школьного возраста)

Люди – рабы своих вещей.
Т. Дерден

Технологии – это всего лишь инструмент.
Б. Гейтс

Интернет-зависимость (или Интернет-аддикция) – навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета. Интернет-зависимость является широко обсуждаемым вопросом, но её статус как психического расстройства формально не установлен. Эта новая болезнь поражает молодую часть населения, преимущественно подросткового возраста и молодых взрослых. Хоть это заболевание не имеет ничего общего с инфекцией, но распространяется по миру со скоростью эпидемии.

В связи с интенсивной компьютеризацией и «интернетизацией» нашего общества стала актуальной проблема патологического использования Интернета, обозначенная за рубежом ещё в конце 80-х. Речь идёт о так называемой «интернет-зависимости» и зависимости от компьютерных игр. Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет и несущие убытки в случае, если у сотрудников появляется патологическое влечение к пребыванию онлайн.

Интернет делает притягательным:

- возможность анонимных социальных интеракций – здесь особое значение имеет чувство безопасности при осуществлении интеракций, включая использование электронной почты, чатов, ICQ и т. п.;
- возможность для реализации представлений, фантазий с обратной связью – в том числе возможность создавать новые образы «Я»; вербализация представлений и/или фантазий, невозможных для реализации в обычном мире, например, ролевые игры в чатах и т. д.;
- чрезвычайно широкая возможность поиска нового собеседника, удовлетворяющего практически любым критериям – здесь важно отметить, что нет необходимости удерживать внимание одного собеседника – так как в любой момент можно найти нового;
- неограниченный доступ к информации («информационный вампиризм») – занимает последнее место в списке, так как в основном стать зависимым от всемирной паутины подстерегает тех, для кого компьютерные

сети оказываются чуть ли не единственным (а иногда и единственным) средством общения.

Термин «интернет-зависимость» предложил доктор Айвен Голдберг в 1996 году для описания патологической, непреодолимой тяги к использованию Интернета. Голдберг характеризует интернет-зависимость как «оказывающую пагубное воздействие на бытовую, учебную, социальную, рабочую, семейную, финансовую или психологическую сферы деятельности». Автор предпочитал использовать термин «патологическое использование компьютера». В настоящее время данный термин употребляется для более широкой категории, для обозначения патологического использования компьютера вообще, включая виды использования, не относящиеся к социальным, а термин «интернет-зависимость» используется для обозначения патологического использования компьютера для вовлечения в социальные взаимодействия.

Доктор М. Орзак выделила следующие психологические и физические симптомы, характерные для компьютерной или интернет-зависимости:

Психологические симптомы

- хорошее самочувствие или эйфория за компьютером;
- невозможность остановиться;
- увеличение количества времени, проводимого за компьютером;
- пренебрежение семьёй и друзьями;
- ощущения пустоты, депрессии, раздражения не за компьютером;
- ложь работодателям или членам семьи о своей деятельности
- проблемы с работой или учёбой.

Физические симптомы

- синдром капрального канала (туннельное поражение нервных стволов руки, связанное с длительным перенапряжением мышц);
- сухость в глазах;
- головные боли по типу мигрени;
- боли в спине;
- нерегулярное питание, пропуск приёмов пищи;
- пренебрежение личной гигиеной;
- расстройства сна, изменение режима сна.

Интернет-зависимость – это широкий термин, обозначающий большое количество проблем поведения и контроля над влечениями.

Основные *пять типов,* которые были выделены в процессе исследования К. Янг, характеризуются следующим образом:

1. Киберсексуальная зависимость – непреодолимое влечение к посещению порносайтов и занятию киберсексом.

2. Пристрастие к виртуальным знакомствам – избыточность знакомых и друзей в сети.

3. Навязчивая потребность в сети – игра в онлайновые азартные игры, постоянные покупки или участия в аукционах.

4. Информационная перегрузка (навязчивый web-серфинг) – бесконечные путешествия по сети, поиск информации по базам данных и сайтам.

5. Компьютерная зависимость – навязчивая игра в компьютерные игры.

Советы по предотвращению развития компьютерной зависимости у детей и подростков:

- Так как первопричиной ухода ребёнка из реального мира является неудовлетворённость существующей действительностью, необходимо в первую очередь выяснить, что же побудило ребёнка уйти «в компьютер».
- Неправильно критиковать ребёнка, проводящего слишком много времени за компьютером.
- Если вы видите у ребёнка признаки компьютерной зависимости, не обостряйте ситуацию, отведите его к психотерапевту.
- Можно попытаться вникнуть в суть игры, разделив интересы ребёнка, это сблизит ребёнка с родителями, увеличит степень доверия к ним.
- Рекомендуется ограничивать доступ детей к играм и фильмам, основанным на насилии.

Рекомендуем провести урок для обучающихся среднего школьного возраста в рамках данной содержательной линии в **форме**:

- *тренинга* «Компьютер – друг или враг», «А ты зависим от Интернета?»[1];
- *круглого стола* «Почему люди уходят в виртуальный мир?»;
- *дебатов*, *дискуссии* «Реальность против виртуальности»;
- *встречи с психологом* «Поговорим о проблеме откровенно» и т. д.;
- *урока-визуализации*, в рамках которого можно представить в различных техниках изобразительного искусства, фотографии, декоративно-прикладного творчества подростка, страдающего интернет-зависимостью, и пути её преодоления;
- *защиты проекта* «Неделя / месяц без Интернета»;
- *урока-сказкотерапии*, на котором дети вместе с педагогом придумают тематическую историю, позволяющую осознать проблему и сделать первые шаги к её решению;
- *интеллектуальной эстафеты* «Навстречу психологическому и физическому здоровью»;
- *выступления агитбригады* «Мы за компьютерную не-зависимость!»;

[1] Приложение 1. Тест-опросник «Интернет-зависимость».

- *съёмки социальной рекламы* «Что такое интернет-зависимость?» с последующим её размещением на сайте образовательной организации или на её странице в социальной сети и т. д.

Кибербезопасность: обеспечение конфиденциальности, целостности и доступности данных

(для обучающихся старшего школьного возраста)

> Мы должны найти баланс между неприкосновенностью частной жизни и использованием данных в рамках общественной безопасности.
>
> С. Наделла

В связи с постоянным расширением интернет-аудитории увеличивается и объём пользовательских данных в сети, ведь сегодня онлайн можно сделать практически всё: от оплаты коммунальных услуг до покупки авиабилетов. Одновременно с этим растёт и количество киберугроз. При этом россияне находятся в большей опасности, чем зарубежные пользователи: по данным Лаборатории Касперского, во втором квартале 2014 года Россия заняла первое место среди стран, в которых пользователи подвергались наибольшему риску заражения через Интернет.

При этом уровень знаний о том, как противостоять киберугрозам не растёт, хотя сегодня в результате взлома аккаунта можно потерять гораздо больше, чем на заре рунета. Многие эксперты считают, что огромное количество пользователей до сих пор пренебрегают элементарными правилами, фактически сводя на нет своей беспечностью все усилия, прилагаемые онлайн-сервисами для повышения безопасности.

Существует ряд правил, которые позволят пользователям защитить себя и свои данные на просторах всемирной паутины.

1. Регулярное обновление операционной системы – это один из самых простых, но в то же время наиболее эффективных способов защиты вашего компьютера. Новейшие версии программного обеспечения исправляют обнаруженные уязвимости и делают работу системы более совершенной. Убедитесь в том, что в вашей операционной системе настроено автоматическое получение обновлений системы безопасности, и не забывайте применять новые настройки, перезагружая компьютер после выполнения обновления.

2. Не торопитесь переходить по ссылкам. Знаете ли вы, что каждый день Google выявляет 9500 вредоносных веб-сайтов? В это число входят взломанные легальные сайты и сайты, специально созданные для распространения вредоносных программ. Всегда относитесь настороженно к ссылкам, по

которым вам предлагают перейти. Не забывайте наводить курсор на ссылку, чтобы посмотреть её полный адрес. Относитесь серьёзно к предупреждающим сообщениям Google. Следите за тем, чтобы ваш межсетевой экран и антивирус имели последнюю версию и были активированы.

3. Обращайте внимание на последние изменения в социальных сетях. Например, Facebook недавно изменил адреса электронной почты, предоставляемые пользователям по умолчанию, их перенесли на домен @facebook.com. Это означает, что спамерам теперь будет намного легче вас найти. Отрегулируйте параметры настроек конфиденциальности (privacy settings) и остерегайтесь спама и фишинговых атак.

4. Придумывайте для всех своих учётных записей в Интернете надёжные пароли, обязательно содержащие буквы, цифры и символы. Лучше выбирать длинные пароли, так как злоумышленникам будет труднее их взломать. Создавайте разные уникальные пароли для важных сайтов, например, таких, как основная электронная почта и система дистанционного банковского обслуживания. Старайтесь не использовать один и тот же пароль на разных сайтах. Если злоумышленники узнают ваш пароль к одному из сайтов, они смогут использовать его для взлома и других ваших учётных записей.

5. Не отключайте защиту, когда играете. Если вы увлекаетесь онлайн-играми, оставляйте активным защитное программное обеспечение. Конечно, важно иметь высокоскоростное соединение без помех, но не ценой безопасности. Лучше включите режим игры «Game Mode» в программе, которая защищает компьютер от сетевых вторжений. Этот режим не нарушает прохождение игры и в то же время обеспечивает достаточный уровень защиты.

6. Оградите себя от файлообменных сайтов и пиратских программ. Лучшее решение – никогда не пользоваться файлообменными сайтами для получения пиратских программ, а вместо этого загружать файлы на сайте разработчика искомого программного обеспечения. Если вы всё же хотите пойти на риск, по крайней мере, необходимо предпринять некоторые меры предосторожности: например, почитать комментарии пользователей перед загрузкой файла. Помните, что многие современные популярные файлообменники имеют довольно точную рейтинговую систему, которая поможет вам узнать мнение других пользователей о нужных вам файлах.

7. Остерегайтесь атак методами социальной инженерии. Киберпреступники ежедневно прочёсывают социальные сети в поисках доступной информации о вас. Используя собранную информацию, они могут, например, отправить вам личное письмо от имени вашего учителя, друга или члена семьи. Вы писали недавно на Facebook о вашем любимом месте для отдыха и получили после этого письмо от одноклассника с описанием лучших мест для летнего отпуска и просьбой дать ссылку на недавнюю статью? Будьте настороже. Всегда следите за тем, что вы говорите в Интернете: раскрывая без

надобности такую личную информацию, как отчества, клички домашних животных и т. п., вы можете помочь преступнику.

8. С осторожностью относитесь к выбору друзей. Что может быть лучше новых знакомств в социальных сетях? Социальные сети и создавались ради онлайн-общения и постоянного поддержания связи с другими людьми. Тем не менее, вы определённо рискуете, если не фильтруете людей, которых допускаете в своё близкое окружение. Если вы получите запрос на добавление в друзья от человека, с которым не общались уже много лет, или от вовсе незнакомой личности, будьте внимательны – это может оказаться социальный бот, пытающийся проникнуть в круг вашего общения. Такие боты часто, пользуясь доверием ваших знакомых в Facebook и Twitter, рассылают от вашего имени электронные письма или уведомления, в которых навязываются какие-либо продукты и распространяют вредоносное ПО.

9. Будьте осторожны при загрузке видео. Онлайн-видео сейчас пользуется большой популярностью, но эта процедура может быть рассадником вирусов. Если у вас нет самого современного видеоплеера, загрузите его из заслуживающего доверия источника. Никогда не устанавливайте программное обеспечение с файлообменных сайтов во время просмотра видео и помните о том, что загрузка видео ни в коем случае не требует запуска исполняемого файла (.exe).

10. Будьте осторожны при использовании точек доступа Wi-Fi. Перед подключением необходимо убедиться, что имя сети Wi-Fi (SSID) принадлежит допустимому источнику. Не подключайтесь к случайным незащищённым сетям Wi-Fi. Это увеличивает риски для безопасности ваших данных. Если это возможно, пользуйтесь сетью Virtual Private Network (VPN). VPN позволяет работать в отдельной защищённой частной сети даже при общедоступном подключении. Вы можете пользоваться приложением типа Hotspot Shield, которое настраивает VPN автоматически (если, конечно, вы доверяете производителю подобного ПО).

С каждым днём киберпреступники становятся всё более изобретательными, поэтому не следует ждать прекращения онлайн-атак. что бы вы н делали, важно предпринять основные меры предосторожности, выполняя вышеизложенные советы и установив, по крайней мере, антивирус и достаточно хороший Firewall.

Начать подобный урок рекомендуем с заполнения *анкеты* «Как вы обеспечиваете свою безопасность в Интернете?» (Приложение 2). Выявленные проблемные вопросы можно рассмотреть в **виде:**

- *тематического заседания клуба «Что? Где? Когда?» / викторины / интеллектуального турнира*;
- *веб-квеста* «Безопасное гиперпространство»;

- *разработки проекта* «Кибервсеобуч»;
- *мастер-класса* «Мой безопасный аккаунт»;
- *встречи со специалистами в области информационных технологий;*
- *публичной презентации шуточных тематических вредных советов;*
- *оформления тематических памяток / информационных уголков / интерактивных плакатов / мультимедийных презентаций* и т. д.

Защита детей и подростков от нежелательного контента
(в рамках родительского всеобуча)

Я бы хотел, чтобы мы построили такой
мир, в котором могли бы
контролировать свою информацию,
владеть ею.

Т. Бернерс-Ли

Практически любую информацию можно найти в сети Интернет в свободном доступе. При всех преимуществах подобной информационной открытости следует отметить и её недостатки. Одним из них является аморальное наполнение некоторых веб-ресурсов. Кроме того, даже на серьёзных сайтах иногда всплывают ролики либо реклама вызывающего характера. В этой связи перед каждым педагогами и родителями рано или поздно встаёт вопрос: как защитить ребёнка от нежелательного контента в Интернете.

Важно донести до ребёнка понимание, что далеко не все веб-сайты в сети безопасны и не все являются тем, чем кажутся. Многие веб-ресурсы по разным причинам транслируют фальшивую информацию или копируют другие сайты в тех или иных неблаговидных целях. Любые факты следует проверять по нескольким разным, желательно уважаемым источникам.

В настоящее время существует множество способов предотвратить посещение детьми нежелательных сайтов, довольно большое количество программ, ограничивающих к ним доступ. В зависимости от степени владения родителями компьютером можно найти различные способы оградить ребёнка от нежелательного контента и других рисков сети, не ограничивая при этом его доступ к огромному количеству полезных образовательных и развлекательных ресурсов в Интернете.

Безопасный поиск позволяет исключать из выдачи результатов сайты с материалами сексуального характера и изображения насилия. Хотя ни один фильтр не обладает абсолютной эффективностью, с помощью безопасного поиска вы можете оградить себя и своих детей от неприемлемого контента.

В принципах сообщества YouTube описано, какие материалы можно, а какие нельзя публиковать на сайте. Тем не менее, некоторым пользователям может показаться неприемлемым определённый контент, даже если он не нарушает установленных правил. В безопасном режиме при поиске видео на YouTube не будут отображаться материалы для взрослых, равно как и любые видео с ограничением по возрасту. Этот фильтр также распространяется на раздел «Похожие видео» и все плейлисты. В безопасном режиме также не отображаются комментарии пользователей, поскольку они могут содержать спорные или неуместные высказывания. Таким образом, безопасный режим на YouTube позволяет скрывать нежелательный и неоднозначный контент согласно выбору пользователя, при этом никакие материалы не удаляются с сайта.

Согласно политике Google Play разработчики обязаны присваивать всем загружаемым приложениям соответствующую возрастную категорию: «для всех», «для детей», «для подростков» и «для взрослых». Пользователи могут настроить доступ к приложениям на своём мобильном устройстве, ограничив его одной или несколькими из указанных категорий, и защитить выбранные возрастные настройки PIN-кодом. Если пользователи находят приложения, которым присвоена неверная категория, они могут сообщить компании об этом, пометив приложение «флажком». Каждое отмеченное приложение будет проанализировано командой Google на соответствие её правилам.

Благодаря одной из стандартных возможностей операционной системы iOS родители могут ограничить доступ ребёнка к ряду выбранных приложений. Также благодаря системе рейтингов, действующих на App Store, в основных настройках можно запретить доступ к приложениям, программам, фильмам и музыке, не предназначенных для возрастной категории ребёнка. Для этого в настройках следует отметить те возрастные категории, доступ к которым будет разрешён.

Целесообразно провести встречу с родителями в рамках всеобуча не в форме традиционной *лекции*, а в форме *мастер-класса или практического занятия*, обязательно с участием специалистов по информатике и информационно-коммуникационным технологиям (можно привлечь старшеклассников, выпускников-студентов специализированных образовательных организаций и т. д.), чтобы каждый из родителей получил и теоретические знания, как обезопасить своего ребёнка от вредного контента, и практические навыки использования перечисленных ресурсов, сервисов, а также названного программного обеспечения.

На занятие с родителями рекомендуем также пригласить педагога-психолога, чтобы он обсудил с аудиторией симптомы и профилактику

интернет-зависимости у детей и подростков, а возможно и провёл тематический тренинг.

Очевидно, что все перечисленные темы для обсуждения невозможно раскрыть в рамках одного урока, но каждая из них является очень актуальной в условиях современного информационного общества, поэтому рекомендуем продолжить их рассмотрение на уроках и внеклассных мероприятиях по информатике, на занятиях в творческих объединениях научно-технической направленности, на классных часах, иных воспитательных мероприятиях, а также в рамках индивидуальной работы с обучающимися, у которых выявлены соответствующие психологические или практические трудности.

Интернет-источники:

1. Азбука информационной безопасности от Лаборатории Касперского [Электронный ресурс] – URL: http://it.sakha.ru/2016/12/11/azbuka-informatsionnoj-bezopasnosti/.
2. Безопасность в Интернете [Электронный ресурс] – URL: https://www.youtube.com/watch?v=kDbZtuN1J3M.
3. Безопасность школьников в сети Интернет [Электронный ресурс] – URL: https://www.youtube.com/watch?v=9OVdJydDMbg.
4. Безопасный Интернет [Электронный ресурс] – URL: https://www.youtube.com/watch?v=QzuM0krC8kQ.
5. Безопасный Интернет. Советы от Google [Электронный ресурс] – URL: https://www.youtube.com/watch?v=9vDfbTTkcUU.
6. Видеоурок «Безопасность в сети Интернет» [Электронный ресурс] – URL: https://www.youtube.com/watch?v=uZdx2yt5XeI.
7. Видеоурок для единого урока по безопасности в сети Интернет [Электронный ресурс] – URL: https://www.youtube.com/watch?v=K1XzMIb-bdE.
8. Дети в Интернете (режиссёр Р. Казарян) [Электронный ресурс] – URL: https://www.youtube.com/watch?v=wKPDBwmcrgA.
9. Детская безопасность в Интернете: технологии и рекомендации в помощь учителям и родителям [Электронный ресурс] – URL: http://www.7ya.ru/article/Detskaya-bezopasnost-v-Internete-tehnologii-i-rekomendacii-v-pomow-uchitelyami-roditelyam-Chast-2/.
10. Онлайн. Безопасный Интернет для школьников и не только [Электронный ресурс] – URL: https://www.youtube.com/watch?v=be57ozTCur8.
11. Онлайн-тест на Интернет-зависимость [Электронный ресурс] – URL: http://www.psyhelp.ru/internet/test.php.

12. Основные правила безопасного Интернета [Электронный ресурс] – URL: https://www.youtube.com/watch?v=cn3YVBOP03Q.

13. Основные правила безопасного Интернета для детей и их родителей [Электронный ресурс] – URL: https://www.youtube.com/watch?v=8w97GutOfYA.

14. Официальный ролик Единого урока безопасности школьников в сети Интернет [Электронный ресурс] – URL: https://www.youtube.com/watch?v=QSKaDf9tvss&list=PLJcUAMea-FtxFpoBZmTU8JxxpEkX7ANHF.

15. Сделайте Интернет безопасным для своих детей [Электронный ресурс] – URL: https://www.google.ru/safetycenter/families/start/#home.

16. Социальная реклама «Безопасный Интернет – детям» [Электронный ресурс] – URL: https://www.youtube.com/watch?v=929km1Y3v9A.

17. Социальный ролик против Интернет-зависимости [Электронный ресурс] – URL: https://www.youtube.com/watch?v=5zQ9iFX2WQQ.

18. Тесты. Интернет-зависимость [Электронный ресурс] – URL: https://sites.google.com/site/kyrsbez/211.

19. Фиксики. Интернет [Электронный ресурс] – URL: https://www.youtube.com/watch?v=BnxCG9DeV6o.

20. Формирование безопасной интернет-среды. Видеоролик для родителей [Электронный ресурс] – URL: https://www.youtube.com/watch?v=u7u6eEWVDco.

21. Цифровая эпидемия. Кибербезопасность [Электронный ресурс] – URL: https://www.youtube.com/watch?v=yR8nEvzcPxc.

Приложение 1

Тест-опросник
Интернет-зависимость

1. Вы используете Интернет, чтобы уйти от проблем или избавиться от плохого настроения?

2. Вы не можете контролировать использование Интернета?

3. Вы чувствуете необходимость находиться в Интернете всё дольше и дольше для того, чтобы достичь удовольствия?

4. Каждый раз вы проводите в Интернете больше времени, чем планировали?

5. После излишней траты денег на оплату соединения вы на следующий день начинаете всё сначала?

6. Вы обманываете членов семьи и друзей, скрывая, сколько времени вы проводите в Интернете и степень вашей увлечённости им?

7. Вы чувствуете беспокойство или раздражение, когда вас отрывают от Интернета?

8. Вы думаете об Интернете, находясь вне сети?

9. Находясь вне сети, вы испытываете подавленность или беспокойство?

10. Вы рискуете лишиться важных взаимоотношений, потерять место работы или учёбы из-за Интернета?

Если вы ответили утвердительно на более чем четыре вопроса и ваше увлечение длится больше года, то следует обратиться за помощью к специалисту.

Приложение 2

Анкета
Как вы обеспечиваете свою безопасность в Интернете?

1. Проверяете ли вы значок безопасного соединения в адресной строке браузера при вводе личных данных в почте, в соцсетях, при совершении онлайн-платежей?

- да
- нет
- затрудняюсь ответить

2. Сталкивались ли вы с ошибкой в сертификате безопасности веб-узла?

- да
- нет
- затрудняюсь ответить

3. Что вы делали при появлении ошибки сертификата безопасности веб-узла?

- закрыл(а) веб-страницу
- продолжил(а) открытие веб-узла
- затрудняюсь ответить

4. Как вы обычно попадаете в почту, социальные сети?

- открываю из закладок браузера
- перехожу со страницы быстрого доступа браузера
- набираю адрес в браузерной строке
- захожу через почтовый клиент, например Outlook
- перехожу на сайт из результатов поиска через поисковую систему
- другое

5. Какие пароли вы используете для своих учётных записей?

- разные пароли для всех учётных записей
- разные пароли для наиболее важных, одинаковые – для остальных учётных записей
- одинаковые пароли для всех учётных записей
- другое

6. Как часто вы меняете пароль от почты (для основного и дополнительного ящика)?

- 1 раз в 3 месяца и чаще
- 1 раз в 6 месяцев
- 1 раз в год и реже
- ни разу не менял(а) пароль

7. Как часто вы меняете пароль от социальных сетей?

- 1 раз в 3 месяца и чаще
- 1 раз в 6 месяцев
- 1 раз в год и реже
- ни разу не менял(а) пароль

8. Какая длина у вашего пароля?

- до 5 символов
- от 6 до 8 символов
- от 9 до 10 символов
- более 10 символов
- затрудняюсь ответить

9. Из каких символов состоит ваш пароль?

- из букв и цифр (abc123)
- из символов, букв и цифр (_abc123)
- из символов и букв (_abc)
- только из цифр (123)
- только из букв (abc)

10. Какие буквы вы используете в пароле?

- строчные и прописные буквы (AbC)
- только строчные буквы (abc)
- только прописные буквы (ABC)

11. Какие сочетания букв вы используете в пароле?

- произвольный набор букв (например, khoohugh)
- придуманное вами слово
- русское слово, набранное латинскими буквами.
- фамилию, имя или отчество (свою или близких)
- несколько слов подряд
- общеупотребляемое слово

- набор букв, расположенный подряд на клавиатуре
- одинаковый набор букв
- другое

12. Где вы храните пароли от почтовых сервисов и социальных сетей?

- помню наизусть
- записываю на бумаге (например, в блокноте)
- сохраняю на компьютере или ноутбуке в электронном виде (например, в документах)
- сохраняю в браузере
- сохраняю в специальном приложении для смартфона или планшета
- делаю скриншот в смартфоне или планшете

13. Как вы восстанавливаете пароль от электронной почты (основного и дополнительного ящика)?

- использую номер телефона для восстановления пароля
- использую секретный вопрос
- использую дополнительный адрес электронной почты
- никогда не восстанавливал(а) пароль электронной почты
- другое

14. Какие меры предосторожности вы соблюдаете при использовании электронной почты (основного и дополнительного ящика)?

- внимательно проверяю адрес ссылки, содержащейся в письме, прежде чем перейти
- не подключаю несколько ящиков к одному почтовому сервису
- ничего не делаю
- использую дополнительный почтовый ящик только для определённых целей / социальных сетей / сайтов / игр
- не читаю / удаляю не читая письма из неизвестных источников

15. Что вы делаете при совершении онлайн-платежей?

- изучаю информацию об онлайн-магазине перед совершением покупок
- избегаю онлайн-магазинов, зарегистрированных на бесплатных хостингах
- использую виртуальную клавиатуру при вводе конфиденциальных данных

- проверяю сертификат подлинности SSL, выданный сайту банка или платёжной системе
- ничего

16. Насколько ваш почтовый аккаунт (основной и дополнительный) защищён от мошенников?

- совершенно не защищён
- скорее не защищён, чем защищён
- ни то, ни другое
- скорее защищён, чем не защищён

17. Насколько ваш аккаунт в социальной сети защищён от мошенников?

- совершенно не защищён
- скорее не защищён, чем защищён
- ни то, ни другое
- скорее защищён, чем не защищён

18. Сталкивались ли вы с кражей пароля от электронной почты (основного и дополнительного ящика)?

- нет, не сталкивался(лась)
- да, один раз
- да, несколько раз
- затрудняюсь ответить

19. Сталкивались ли вы с рассылкой спама из вашего почтового аккаунта?

- да
- нет
- не помню

20. Сталкивались ли вы с кражей пароля от профиля в соцсети?

- нет, не сталкивался(лась)
- да, один раз
- да, несколько раз
- затрудняюсь ответить

21. Сталкивались ли вы с рассылкой спама с вашего аккаунта в соцсети?

- да
- нет
- не помню

22. Получали ли вы мошеннические сообщения в соцсети?

- да
- нет
- не помню

23. Почему вы стали жертвой мошенничества (при пользовании почтой, социальными сетями, при совершении онлайн-платежей)?

- использовал(а) простой пароль
- скачал(а) вирус
- перешёл(шла) по ссылке на мошеннический сайт
- использовал(а) один и тот же пароль на нескольких сервисах
- ответил(а) на мошенническое сообщение
- не разлогинировал(а)ся(сь) при завершении работы в почте, соцсетях