

30 октября 2015 года в МБОУ «СОШ №12» ПГО г. Партизанск прошел тематического урок, посвященный Интернет безопасности детей.

В рамках урока «Интернет-безопасность» в начальных классах обучающихся ознакомили:

1. с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи;
2. как критически относиться к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи, как отличить достоверные сведения от недостоверных, как избежать вредной и опасной для них информации, как распознать признаки злоупотребления их доверчивостью и сделать более безопасным свое общение в сети Интернет;
3. как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей, и избегать выкладывания в сеть компрометирующую информацию или оскорбительные комментарии и т.д.

Ребятам продемонстрированы возможности детских поисковых систем <http://kids.quintura.ru>, <http://agakids.ru> и детского браузера <http://www.gogul.tv>, а также их познакомили с детскими социальными сетями: - <http://cyberpara.ru/>, - <http://interneshka.net/>, - http://kinderonline.ru/detskiy_portal.html, - <http://1dnevnik.ru/>, - <http://www.detkino.ru>.

При проведении урока были использованы материалы сайта www.dettonline.com (видеоматериалы, материалы электронного 7 журнала «Дети в информационном обществе», материалы Линии помощи).

Урок проводился в форме викторины.

При проведении использовались ссылки:

- 1) http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/loputon_metsa.html – о правилах безопасного поведения в сети Интернет с элементами интерактива;
- 2) <http://www.nachalka.com/node/948> - учебное видео «Как обнаружить ложь и остаться правдивым в Интернете»;
- 3) <http://content-filtering.ru/aboutus/> - информационно-аналитический ресурс «Ваш личный Интернет».

Основная школа (5 - 7 и 8 - 9 классы)

В ходе урока «Интернет-безопасность» в среднем звене обучающихся познакомили с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве:

- Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (Закон определяет информационную безопасность детей как состояние защищенности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.);

- № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»,

(направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребёнке порочные наклонности, сформировать у ребёнка искажённую картину мира и неправильные жизненные установки.)

Ознакомили обучающихся с адресами помощи в случае интернет- угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015).

Урок был проведен в форме беседы «10 правил безопасности в интернете».

В начале урока учащимся показали видео, где объясняются основные правила безопасности в интернете - <http://www.youtube.com/watch?v=wVDsCpYSpeo>
Каждый современный человек, ежедневно проводит время в интернете. Но интернет — это не только источник информации и возможность общаться на расстоянии, но и угроза компьютерной безопасности. Вы можете скачать из сети компьютерный вирус, Вашу учетную запись или адрес электронной почты, могут взломает злоумышленник.

Правила безопасности в интернете.

1) Используйте надежный пароль. Первое и главное правило сохранности Ваших данных, учетных записей, почтовой пересылки это надежный пароль! Много раз хакеры взламывали страницы в социальных сетях или почтовые адреса из-за того, что пользователь ставил простой пароль. Вы ведь не хотите, чтобы Ваши личную переписку узнал кто-то чужой? Используйте генератор паролей, чтобы получить надежный пароль. Генератор паролей создается, чтобы помочь вам с придумыванием устойчивых к взлому и легко запоминающихся паролей. Часто бывает: вы зарегистрировались где-нибудь, а там просят: «введите пароль». В спешке приходится вводить что-нибудь типа qwerty или 11 12345. Последствия могут быть фатальными для вашего аккаунта: при попытке взлома такие пароли проверяются в первую очередь. Чтобы этого не происходило, надо создавать сложный пароль, желательно состоящий из букв разного регистра и содержащий цифры и другие символы. Для создания таких паролей существуют специальные программы. Но, на наш взгляд, гораздо легче набрать наш адрес и просто выбрать понравившийся пароль. Советы: - Выбирайте пароль посложнее, состоящий из символов разного регистра, с цифрами и для абсолютной надёжности - знаками препинания. - Не используйте пароль, связанный с теми данными, которые могут быть о вас известны, например, ваше имя или дату рождения. - Пароли, которые вы видите на экране создаются в реальном времени на вашем компьютере, поэтому исключена возможность перехвата пароля по сети. Разные посетители сайта видят разные пароли. Если вы зайдете на сайт второй раз, пароли будут другими. - Вы можете выбрать пункт меню браузера "Файл|Сохранить как...", чтобы пользоваться генератором паролей в оффлайне. - Генератор паролей полностью прозрачен: скачайте файл passwd.js, чтобы увидеть, как создается пароль, и убедиться в абсолютной надёжности. Источник- <http://genpas.narod.ru/>

2) Заходите в интернет с компьютера, на котором установлен фаервол или антивирус с фаерволом. Это в разы уменьшит вероятность поймать вирус или зайти на вредоносный сайт.

3) Заведите один основной почтовый адрес и придумайте к нему сложный пароль. При регистрации на форумах, в соц. сетях и прочих сервисах Вы будете указывать его. Это необходимо если Вы забудете пароль или имя пользователя. Ни в коем случае не говорите, никому свой пароль к почте, иначе злоумышленник сможет через вашу почту получить доступ ко всем сервисам и сайтам, на которых указан Ваш почтовый адрес.

4) Если Вы хотите скачать какой-то материал из интернета, на сайте где не нужна регистрация, но от Вас требуют ввести адрес своей электронной почты, то, скорее всего, на Ваш адрес будут высылать рекламу или спам. В таких случаях пользуйтесь одноразовыми почтовыми ящиками.

5) Скачивайте программы либо с официальных сайтов разработчиков. Не скачивайте программы с подозрительных сайтов или с файлообменников. Так Вы уменьшите риск скачать вирус вместо программы.

6) Не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они не были. В лучшем случае, Вы поможете автору сайта получить деньги, а в худшем — получите вирус. Используйте плагины для браузеров, которые отключают рекламу на сайтах.

7) Если Вы работаете за компьютером, к которому имеют доступ другие люди (на работе или в интернет кафе), не сохраняйте пароли в браузере. В противном случае, любой, кто имеет доступ к этому компьютеру, сможет зайти на сайт, используя Ваш пароль.

8) Не открывайте письма от неизвестных Вам пользователей (адресов). Или письма с оповещением о выигрыше в лотереи, в которой Вы просто не участвовали.

9) Не нажимайте на всплывающие окна, в которых написано, что Ваша учетная запись в социальной сети заблокирована. Это проделки злоумышленников! Если Вас вдруг заблокируют, Вы узнаете об этом, зайдя в эту социальную сеть, или администрация отправит Вам электронное письмо.

10) Периодическим меняйте пароли на самых важных сайтах. Так Вы уменьшите риск взлома вашего пароля. Пользуясь этими правилами безопасности в интернете, Вы существенно уменьшите риск получить вирус на свой компьютер или потерять учетную запись на любимом сайте.

Далее ребята обсудили и дополнили 10 основных правил.

Для обучающихся 8-9 классов прошло занятие «Киберугрозы современности: главные правила их распознавания и предотвращения» в форме семинара. Целью стало расширение знаний о киберугрозах, формирование навыков их распознавания и оценки рисков.

Занятие началось показом социального видеоролика «Безопасный интернет - детям!»

(http://www.youtube.com/watch?v=9uvNVZMdeIk&feature=player_embedded).

После просмотра ролика и объявления темы занятия ученики сами сформулировали цель занятия.

Полезные ссылки:

- 1) http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/ryhma_roma.html - молодёжная история с элементами интерактива;
- 2) <http://content-filtering.ru/aboutus> - информационно-аналитический ресурс «Ваш личный Интернет»;
- 3) www.icensor.ru – Интернет-фильтр.

Старшая школа (10 - 11 классы).

В рамках урока «Интернет-безопасность» в старших классах обучающихся познакомили с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве. Обратить внимание обучающихся на классификацию вредоносных информационных ресурсов:

- информация, причиняющая вред здоровью и (или) развитию детей;
- информация, запрещенная для распространения среди детей;
- информация, ограниченная для распространения среди детей определенных возрастных категорий.

На уроке были затронуты следующие аспекты:

- перечень рисков, подстерегающих ребенка в сети Интернет;
- рекомендации по грамотному использованию электронной почты;
- технологии безопасного общения в средах мгновенного обмена сообщениями.

Обучающимся раздали: - инструкции по безопасному общению в чатах; - советы по профилактике и преодолению Интернет- зависимости; - общие правила по безопасности детей в сети Интернет.

Также были рассмотрены следующие объекты, являющиеся опасными в Интернете:

- нежелательные программы;
- защита личных данных;
- мошенничество;
- виртуальные «друзья»;
- пиратство;
- on-line-игры; - этика;
- критический подход к информации.

Обучающимся познакомили с информацией о программном обеспечении, позволяющим осуществлять безопасную работу в сети Интернет, контентной фильтрации, а также ознакомить с адресами помощи в случае интернет-угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015).

Урок был проведен в форме мозгового штурма «Интернет-безопасность».

Полезные ссылки: 1) <http://www.kaspersky.ru> – антивирус «Лаборатория Касперского»; 2) <http://www.onlandia.org.ua/rus/> - безопасная web-зона; 3) <http://www.interneshka.net> – международный онлайн-конкурс по безопасному использованию Интернета; 4) <http://www.saferinternet.ru> – портал Российского Оргкомитета по безопасному использованию Интернета; 5)

filtering.ru – Интернет СМИ «Ваш личный Интернет»; 6) <http://www.rgdb.ru> –
Российская государственная детская библиотека.

При подготовке урока, посвященного интернет безопасности школьников, использовались следующие материалы:

1. Электронные ресурсы по теме «Безопасный Интернет» 1. <http://www.saferinternet.ru/> - Безопасный Интернет. Портал Российского Оргкомитета по проведению Года Безопасного Интернета. Мероприятия, Интернет и законодательство, проблемы и решения, международные ресурсы;
2. <http://www.saferunet.ru/> - Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Интернет-угрозы и эффективное противодействием им в отношении пользователей;
3. <http://www.fid.su/> - Фонд развития Интернет. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета;
4. <http://www.microsoft.com/Rus/athome/security/kids/etusivu.html> - Безопасность в Интернете. "Основы безопасности детей и молодежи в 30 Интернете" — интерактивный курс по Интернет-безопасности, предлагаемый российским офисом Microsoft в рамках глобальных инициатив Microsoft "Безопасность детей в Интернете" и "Партнерство в образовании". В разделе для учащихся (7-16 лет) предлагается изучить проблемы информационной безопасности посредством рассказов в картинках. В разделе для родителей и учителей содержится обновленная информация о том, как сделать Интернет для детей более безопасным, а также изложены проблемы компьютерной безопасности;
5. http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=cs_teach_kids – Club Symantec единый источник сведений о безопасности в Интернете. Статья для родителей «Расскажите детям о безопасности в Интернете». Информация о средствах родительского контроля;
6. <http://www.nachalka.com/bezopasnost> - Nachalka.com предназначен для учителей, родителей, детей, имеющих отношение к начальной школе. Статья «Безопасность детей в Интернете». Советы учителям и родителям;
7. <http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html> - Личная безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать посещение Интернета для детей полностью безопасным;
8. <http://www.ifap.ru/library/book099.pdf> - «Безопасность детей в Интернете», компания Microsoft. Информация для родителей: памятки, советы, рекомендации;
9. <http://www.interneshka.net/children/index.phtml> - «Интернешка» - детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». Регистрация и участие в конкурсе по безопасному использованию сети Интернет;
10. <http://www.oszone.net/6213/> - OS.zone.net - Компьютерный информационный портал. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль»;
11. <http://www.rgdb.ru/innocuous-internet> - Российская государственная детская библиотека. Ресурс для детей и родителей. Правила безопасного Интернета. Обзор программных продуктов для безопасного Интернета. Как защититься от Интернет-угроз. Ссылки на электронные ресурсы, информирующие об опасностях и защите в Сети;
12. <https://www.google.ru/safetycenter/families/start/basics/> - Центр безопасности.

Краткие рекомендации помогут обеспечить безопасность членов семьи в Интернете, даже если вечно не хватает времени; 31 13. <https://ege.yandex.ru/security/> - Тесты по безопасности; 14. <http://www.slideshare.net/shperk/ss-47136465> - Безопасность в Интернете. Анатолий Шперх; 15. <http://shperk.ru/v-seti/prokrustovo-lozhe.html> - Прокрустово ложе для информационной картины. Как мы читаем тексты в интернете; 16. <http://shperk.ru/sovety/avtoritet.html> - Как отличить фейк от настоящего материала? Дело о летающем дьяке Крякутном; 17. <http://habrahabr.ru/company/mailru/blog/252091/> - Советы по безопасности