2

СЦЕНАРИЙ РАБОТЫ УЧИТЕЛЯ,

направленный на формирование у обучающихся
гражданско-патриотических ценностей

ИНФОРМАТИКА

Занятие с использованием приема «Разворачивающаяся кооперация» по теме: «ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ»

5-9 классы

Предмет: Информатика

Класс: 9

Тема: Информационное общество: нормы информационной этики и права; информационная безопасность

Формирующиеся ценности: нравственность, гражданственность.

Планируемые результаты:

Личностные:

ориентация на моральные ценности и нормы в ситуациях нравственного выбора; готовность оценивать свое поведение и поступки, а также поведение и поступки других людей с позиции нравственных и правовых норм с учетом осознания последствий поступков; активное неприятие асоциальных поступков, в том числе в сети Интернет;

представление о социальных нормах и правилах межличностных отношений в коллективе, в том числе в социальных сообществах; соблюдение правил безопасности, в том числе навыков безопасного поведения в интернет-среде; готовность к разно образной совместной деятельности при выполнении учебных, познавательных задач, создании учебных проектов; стремление к взаимопониманию и взаимопомощи в процессе этой учебной деятельности.

Метапредметные:

умение определять понятия, создавать обобщения, делать умозаключения и выводы;

сопоставлять свои суждения с суждениями других участников диалога, обнаруживать различие и сходство позиций;

публично представлять результаты выполненного опыта (эксперимента, исследования, проекта);

понимать и использовать преимущества командной и индивидуальной работы при решении конкретной проблемы, в том числе при создании информационного продукта; 6 принимать цель совместной информационной деятельности по сбору, обработке, передаче, формализации информации; коллективно строить действия по ее достижению: распределять роли, договариваться, обсуждать процесс и результат совместной работы.

Предметные:

соблюдать сетевой этикет, базовые нормы информационной этики и права при работе с приложениями на любых устройствах и в сети Интернет, выбирать безопасные стратегии поведения в сети;

защищать персональную информацию от несанкционированного доступа и его последствий (разглашения, подмены, утраты данных) с учетом основных технологических и социально-психологических аспектов использования сети Интернет (сетевая анонимность, цифровой след, аутентичность субъектов и ресурсов, опасность вредоносного кода);

распознавать попытки и предупреждать вовлечение себя и окружающих в деструктивные и криминальные формы сетевой активности (в том числе кибербуллинг, фишинг).

Продолжительность: 25 мин.

Необходимые средства: компьютерный класс; установленный на компьютеры офисный пакет с текстовым процессором и редактором презентаций.

СЦЕНАРИЙ РАБОТЫ

Девятиклассники, как правило, имеют богатый опыт использования разнообразных ресурсов и сервисов сети Интернет. Задача учителя – актуализировать, расширить и систематизировать знания учеников в области информационной этики и права. Свод основных правил.

Для вовлечения школьников в активное обсуждение правил безопасного поведения в сети Интернет может быть использован прием «Разворачивающаяся кооперация».

1. Учитель просит каждого ученика подумать и записать (ручкой на листке бумаги; создав документ в текстовом процессоре) 2–3 правила безопасного поведения в сети Интернет; на работу отводится 2–3 минуты.
2. Далее учитель предлагает учащимся объединиться в пары и составить общий список правил безопасного поведения в сети Интернет. При этом одинаковые или похожие ответы объединяются, а по поводу несовпадений ребятам придется договориться. На эту работу паре отводится до 5 минут.
3. Далее школьники объединяются в команды по четыре человека и составляют общий для них список правил.
4. Следующий этап – четверки объединяются в восьмерки и проделывают ту же работу. Объединение в группы желательно закончить на этапе, когда в классе сформировалось 2 или 3 команды обучающихся.
5. Учитель собирает списки, подготовленные группами (в бумажном или электронном формате), и просит выбрать из каждой группы одного человека – эксперта, которому предстоит оценить работу другой группы.
6. Учитель поочередно выводит на экран заранее подготовленные правила, а эксперты, получившие ответы других команд, фиксируют, есть ли среди ответов команд совпадения с теми правилами, на которые обращает внимание учитель. По числу таких совпадений выбирается команда, сумевшая сформировать наиболее полный ответ.

ПРИЛОЖЕНИЕ

Правила безопасного поведения в сети Интернет

Создавая свой профиль в социальных сетях, не указывайте свой адрес, дату рождения, школу, класс. Придумывая себе логин (ник, имя пользователя), вместо имени используйте псевдоним; вы можете отразить в нем свои стремления, характер, интересы. При этом личную информацию, такую как ваша фамилия или дата рождения, включать в логин не рекомендуется.

Пароли должны быть уникальными; цифры и спецсимволы значительно усложняют процесс их подбора злоумышленниками. В социальные сети, мессенджеры и почту безопаснее входить через приложения; ввода паролей в браузерах следует избегать. Не пользуйтесь сервисами, которые сохраняют пароли: онлайн-сервисы для хранения паролей ненадежны; их часто взламывают. Никому не сообщайте свои пароли. При завершении работы с общедоступным компьютером корректно выходите из учетных записей, которые вы использовали.

Будьте особенно бдительны при совершении интернет-покупок, согласовывайте все платежи с родителями. Обратите внимание на строку браузера на странице, на которой вводятся платежные данные; проверьте, есть ли в строке браузера изображение закрытого навесного замочка — он означает безопасную передачу данных. Когда замочек открыт, защита недостаточна. Если есть изображение восклицательного знака или перечеркнутого замка, на таком сайте не стоит вводить свои данные.

Свои персональные данные (фамилию, домашний адрес, номер телефона, название школы, номера документов и т. д.) можно вводить только на государственных сайтах или на сайтах для покупки билетов. И только в том случае, если соединение устанавливается по протоколу HTTPS. Не оставляйте свои персональные данные на других сайтах.

Учитесь различать оригинальные и поддельные сайты. Поддельные сайты могут иметь дизайн и адрес, напоминающие сайт-оригинал. Злоумышленники ждут, когда человек введет логин и пароль на поддельном сайте. Узнав эти данные, они используют их для входа в настоящий профиль своей жертвы.

Старайтесь не выкладывать полную информацию (фотографии, видеозаписи) о себе и жизни своей семьи на всеобщее обозрение. Доступ к такой информации можно открывать только проверенным людям: родным, близким, друзьям и людям, с которыми вы знакомы в реальной жизни. Помните: все, что попало в Сеть, останется там навсегда. Как правило, стереть данные из Сети невозможно. Единственный способ избежать утечки информации — не делиться ею без особой на то необходимости.

Особенно внимательно ведите себя в онлайн-играх: игровые объекты, членство в командах, социальные связи внутри игры — все это может стать механизмом манипуляции для мошенников и других злоумышленников. В Интернете много сайтов, содержащих аркады, головоломки, другие игры с системой начисления очков; здесь деньги не тратятся. Сайты с азартными играми, как правило, связаны с выигрышем или проигрышем денег. Привычка к азартным играм приводит к формированию у человека психологической зависимости, представляющей серьёзную социальную и медицинскую проблему.

Поскольку каждый пользователь Интернета может опубликовать любую информацию, не все, что вы видите в Сети, верно. Старайтесь мыслить критически, чтобы оценить достоверность материалов. При поиске информации по интересующему вас вопросу обращайте внимание на источник информации, отдавая предпочтение официальным сайтам. Сверяйте найденную в Сети информацию по 2–3 источникам; проверяйте, есть ли в Сети другие мнения и факты, которые противоречат ранее найденной вами информации. Не доверяйте безоговорочно сайтам с кричащими заголовками и обилием рекламы; следует насторожиться, если пользователя, щелкнувшего на какой-либо новости, перекидывают куда-то дальше. Не посещайте сайты расистского, дискриминационного, насильственного содержания — они способны поставить под угрозу психологическое и физическое здоровье молодого человека.

Соблюдайте сетевой этикет. Не старайтесь привлечь к себе внимание за счет эпатажа. Пишите грамотно. Не оскорбляйте других, не будьте навязчивы, не позволяйте своим негативным эмоциям выходить из-под контроля. Получив оскорбительное или иное сообщение, заставляющее вас чувствовать себя некомфортно, не отвечайте на него. Никогда не участвуйте в травле: буллинг в Сети ничем не отличается от реального и одинаково опасен и для жертвы, и для агрессора.

Онлайн-друг может быть совсем не тем человеком, за кого он себя выдает. Злоумышленники, выдавая себя за вашего сверстника, могут пытаться выведать частную информацию о вас и членах вашей семьи. Затем, в зависимости от своих целей, они могут искать личной встречи, угрожать жертве. Прежде чем вступить в диалог с незнакомцем, обратите внимание на его возраст и число друзей в Сети; следует насторожиться, если незнакомец старше вас, имеет очень мало друзей, просит вас выслать ему какие-нибудь фото или данные, — это явные приметы злоумышленника.

Фишинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей. Опасайтесь интернет-мошенничества: получив сообщение о выигрыше или возможности бесплатного получения какой-то вещи, не вводите пароли, номера телефонов, банковских карт или другую личную информацию. Помните: подлинные интернет-сервисы не

рассылают пользователям писем с просьбами сообщить свои учётные данные, пароль и прочее.

- Многие веб-сайты предлагают пользователям для бесплатного скачивания различные приложения, игры, музыку, фильмы, документы, которые могут содержать вирусы. Избежать заражения вирусами помогают антивирусные программы.

- Позаботьтесь о безопасности копий важных документов, которые вы решили хранить в облаке. Отсканированные документы поместите в архив, при создании которого выберите опцию «непрерывный архив» (*solid archive*) и установите для этого архива пароль. Не используйте один и тот же пароль для разных архивов.

- Избегайте любых деструктивных и криминальных форм сетевой активности.