Государственное бюджетное профессиональное
образовательное учреждение Республики Марий Эл
«Йошкар-Олинский строительный техникум»

МЕТОДИЧЕСКАЯ РАЗРАБОТКА

внеклассного мероприятия Информационный час с викториной,

посвященного «Субботе правовой грамотности» в рамках научно-познавательных и культурных суббот «Калейдоскоп открытий»

Тема: Правила общения в сети Интернет и юридическая ответственность за их нарушения

Авторы:
1. Удалова Марина Николаевна,
преподаватель юридических дисциплин
ГБПОУ Республики Марий Эл
«Йошкар-Олинский Строительный техникум»
2. Щеглова Наталья Валерьевна,
преподаватель юридических дисциплин
ГБПОУ Республики Марий Эл
«Йошкар-Олинский Строительный техникум»
высшей квалификационной категории

г.Йошкар-Ола
2022

ПЛАН ПРОВЕДЕНИЯ ВНЕКЛАССНОГО МЕРОПРИЯТИЯ

Тема: «Правила общения в сети Интернет и юридическая ответственность за их нарушения».

Цели: 1. Формирование правовой грамотности.

2. Популяризация знаний о правах и обязанностях гражданина Российской Федерации, Республики Марий Эл перед государством и обществом.

3. Профориентация, направленная на подготовку обучающихся к выбору профессии в юридической отрасли.

Задачи:

Образовательные:

1. Изучить основные правила общения в сети Интернет.

2. Ознакомить обучающихся с нормами уголовного и административного законодательства, регулирующими правоотношения в сети Интернет.

3. Сформировать представление обучающихся об основных интернет-угрозах и способах их предотвращения.

Воспитательные:

1. Содействовать формированию у обучающихся способности и готовности к безопасному и ответственному использованию Интернет-ресурсов.

2. Развить способности обучающихся к сотрудничеству, общению и работе в коллективе.

3. Содействовать повышению правовой культуры обучающихся.

4. Создать предпосылки для возможного дальнейшего профессионального выбора подростков, пробудив познавательный интерес к юридическим специальностям.

Развивающие:

1. Способствовать развитию творческих способностей, коммуникативных навыков обучающихся.

2. Развить у детей самостоятельность и инициативность.

Межпредметные связи: информатика, обществознание.

Ожидаемые результаты мероприятия:

1. Знание основных правил общения в сети Интернет.

2.Знакомство с нормами уголовного и административного законодательства, регулирующими правоотношения в сети Интернет.

3. Знание основных интернет-угроз и способов их предотвращения.

4. Умение работать в коллективе, решение игровых задач.

5. Привить обучающимся интерес к специальности «Правоохранительная деятельность» и «Право и организация социального обеспечения».

Форма проведения мероприятия – беседа, викторина.

Участники: обучающиеся 9, 10 и 11 классов МОУ Средней общеобразовательной школы № 3 п. Советский Советского района Республики Марий Эл – 30 человек.

Место проведения: читальный зал ГБПОУ Республики Марий Эл «Йошкар-Олинский строительный техникум».

Оборудование: проектор, экран, звуковая аппаратура и ноутбук.

Время проведения: 90 минут.

Этапы мероприятия:

1. Вступительное слово преподавателя. Постановка темы мероприятия.

2. Информация о безопасном общении в сети Интернет.

2.1. Правила безопасного поведения в системе Интернет.

2.2. Правонарушения в системе Интернет и ответственность за их совершение.

3. Проведение викторины.

4. Заключительное слово преподавателя, подведение итогов, награждение.

Ход занятия.

1. Вступительное слово преподавателя. Постановка темы мероприятия.

Добрый день! Ребята, как вы думаете, почему наша тема звучит как «Правила общения в сети Интернет и юридическая ответственность за их нарушения»?

Выслушать ответы обучающихся.

Интернет стал неотъемлемой частью нашей жизни, но информационное пространство не является нерегулируемой системой. Отношения между людьми регулируются законами РФ: Конституцией, Кодексом об Административных правонарушениях, Уголовным кодексом и другими законами. Для Интернета, как системы обмена информацией, принят свой ряд законов. Сегодня мы с вами поговорим о том, что можно и чего нельзя в интернете. Если вовремя и откровенно не обсудить правила безопасности в сети Интернет в вашей жизни и жизни ваших близких могут возникнуть неприятные и самые неожиданные моменты, которые принесут массу неприятностей и могут сыграть трагичную роль.

Как же обеспечить информационную безопасность? Сегодня мы с вами об этом и поговорим.

Дети начинают проявлять интерес к социальным сетям в уже возрасте 10-16 лет. Они открывают для себя самые популярные площадки: Вконтакте, Телеграмм, Инстаграмм, Одноклассники и, не задумываясь о простых правилах, смело выкладывают подробную информацию о себе, обмениваются номерами телефонов и адресами, электронной почтой.

Очень часто юные пользователи не понимают, что на их страничку в соцсетях могут зайти не только друзья, но и те, кто под видом друзей может причинить массу неприятностей. В результате возникают проблемы: административные правонарушения, троллинг, сетевая травля, психологическое давление, которое может стать причиной комплексов, неуверенности в себе и даже совершаются уголовные преступления.

А если вы сами ведете себя в сети Интернет неэтично, то своими действиями можете совершить правонарушения.

2. Информация о безопасном общении в сети Интернет.

2.1. Правила безопасного поведения в системе Интернет.

Презентация (прилагается).

Семь правил безопасного поведения в Интернете.

1) Храните тайны!

В информационном пространстве нам часто приходится вводить свои данные. Безопасно ли это?

Персональные данные (имя, фамилия, адрес, дата рождения, номера документов) можно вводить только на государственных сайтах или на сайтах

покупки билетов. И только в том случае, если соединение устанавливается по протоколу https. Слева от адреса сайта должен появиться значок в виде зеленого замка — это означает, что соединение защищено.

2) Сохраняйте анонимность!

Создавая свой профиль в социальных сетях, нужно максимально избегать привязки к «физическому» миру.

Нельзя указывать свой адрес, дату рождения, школу, класс. Лучше использовать очевидный псевдоним: по нему должно быть ясно, что это не настоящее имя (ведь использовать ложные данные: «Алексей» вместо «Александр» — по правилам соцсетей запрещено).

3) Не разговаривайте с незнакомцами!

Есть несколько главных опасностей, с которыми можно столкнуться в Интернете. По большому счету они мало отличаются от тех, что угрожают нам в реальной жизни. Злоумышленники здесь просто используют другие средства.

4) Распознайте злоумышленника!

На что надо обратить внимание прежде, чем вступить в диалог? Что сигнализирует об опасности?

Вы не знакомы с этим человеком в реальной жизни. У него нет или очень мало друзей в соцсети. Собеседник о чем-то просит: сфотографироваться, прислать какие-то данные и т.д.

5) Не сообщайте своё местоположение!

Данные геолокации позволяют всему миру узнать, где вы живете и учитесь, проводите свободное время, в каких акциях участвуете, какие шоу и спектакли любите, как отдыхаете. Отследить местоположение человека теперь не составляет труда.

6) Учитесь замечать поддельные сайты!

Фишинг — это способ выманивать у человека его данные: логин, название учетной записи и пароль.

Происходит это так: пользователю присылают ссылку на сайт, очень похожую на настоящий адрес почтового сервиса или социальной сети. Как правило, фишеры специально покупают такие домены. Например, для mail.ru это может быть «meil.ru», а для vk.com — «vk-com.com».

Злоумышленник ждет, когда человек введет логин или пароль на поддельном сайте. Так он узнает данные, а потом использует их для входа в настоящий профиль своей жертвы.

7) Главный секрет безопасности в сети Интернет - не нужно делать в Интернете ничего, что бы вы не стали бы делать в физическом мире. Разница между виртуальной и реальной действительностью минимальна.

2.2. Правонарушения в системе Интернет и ответственность за их совершение.

А сейчас давайте поговорим о правонарушениях при общении в системе Интернет и об ответственности за собственное поведение.

МОШЕННИЧЕСТВО, то есть хищение чужого имущества путем обмана или злоупотребления доверием (ст.159 УК РФ). Наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет.

Через Интернет могут предложить приобрести все, что угодно, а распознать подделку при покупке через сеть бывает сложно.

Фишинг.

Вид интернет-мошенничества, цель которого – получить данные, содержащиеся на вашей пластиковой карте. Злоумышленники рассылают электронные письма от имени банков или платежных систем. Пользователю предлагается зайти на сайт, который является точной копией настоящего сайта банка, где можно увидеть объявления, например, об изменении системы безопасности банка. Для дальнейшей возможности использовать свою пластиковую карту просят указать пин-код и данные, содержащиеся на карте. Впоследствии эти данные используются для изготовления поддельной пластиковой карты и обналичивания денежных средств, содержащихся на вашем счете.

Интернет-попрошайничество.

В Интернете могут появляться объявления от благотворительной организации, детского дома, приюта или просто от родителей с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-

дублер, который является точной копией настоящего, меняют реквизиты для перечисления денег.

Вирусы.

Сущность вируса – переадресация со страницы запрашиваемого ресурса на фиктивную, скопированную с настоящей. Подмена осуществляется для самых популярных ресурсов Рунета: Яндекс, Рамблер, Майл, ВКонтакте, Одноклассники. Набирая на «зараженном» компьютере адрес одного из указанных ресурсов, пользователь попадает на сервер-подмену, где ему предлагается страница для входа в систему (имя и пароль). С учетом того, что в адресной строке указано корректное имя, а внешний вид скопирован с оригинального сервера, у большинства пользователей не возникает подозрений в подлинности страницы. После ввода имени и пароля отображается иная страница, где уже говорится о необходимости «подтверждения» или «активации» учетной записи за смс на короткий номер, стоимость которого минимальная или якобы бесплатная. Таким образом, злоумышленники не только снимают денежные средства со счетов абонентов, но и получают логин и пароль доступа пользователя к указанным популярным ресурсам, что позволяет им в дальнейшем отправлять от имени «жертвы» различные сообщения,

ОСКОРБЛЕНИЕ, КЛЕВЕТА, БУЛЛИНГ.

Оскорбление — унижение чести и достоинства личности, выраженное в неприличной форме или иной противоречащей общепринятым нормам морали и нравственности форме.

За оскорбление, совершенное публично с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет» установлена административная ответственность по статье 5.61 Кодекса РФ об административных правонарушениях, влечет наложение административного штрафа на граждан в размере от 5000 рублей до 10000 рублей.

Например, гр.А. в одной из групп «В контакте» в сети «Интернет» под фотографией гр.Б. разместил нецензурное выражение, оскорбляющее его достоинство. Факт получения сообщения подтверждается скриншотом, который в последующем прилагается к заявлению. Стоит обратить внимание, что сообщение может быть и правдивым, но выражено в грубой и неприличной форме.

Оскорбление — с 15 января 2021 года это унижение чести и достоинства не только в неприличной форме, но и в любой другой, если она противоречит нормам морали. Формулировка непонятная и без конкретики,

так что штраф могут назначить не только за слова, но и, например, за неприличный жест или картинку.

Также оскорблением или клеветой может быть признана информация, содержащаяся в видеороликах, карикатурах, демотиваторах, мемах и гифках.

Клевета — распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию.

Например, гр.А. разместил в сети Интернет порочащую и не соответствующую действительности информацию, относящуюся к гр-ну Б. Другие лица могли прочитать эту ложную и порочащую информацию. Совершенное деяние предусмотрено ст.128.1 УК РФ - клевета, содержащаяся в публично демонстрирующихся средствах массовой информации либо совершенная публично с использованием информационно-телекоммуникационных сетей, включая сеть "Интернет», наказывается штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до двухсот сорока часов, либо принудительными работами на срок до двух лет, либо арестом на срок до двух месяцев, либо лишением свободы на срок до двух лет.

Фейки — это искаженная или лживая, не соответствующая действительности, вводящая в заблуждение, поддельная информация. При этом она никого не оскорбляет, но угрожает жизни и имуществу, общественной безопасности или работе важной инфраструктуры.

В соответствии с частью 9 ст. 13.15 Кодекса об административных правонарушениях Российской Федерации распространение в средствах массовой информации и на сайтах сети Интернет заведомо недостоверной общественно значимой информации под видом правдивых фактов может повлечь административную ответственность в виде штрафа в размере до 100 тыс. руб. для граждан.

В силу части 10.1 ст. 13.15 Кодекса об административных правонарушениях Российской Федерации распространение в средствах массовой информации и Интернете информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, наступает ответственность в виде штрафа в размере до 3 млн. руб.

Буллинг. Зачастую злоумышленнику становятся известны анкетные данные подростка, и тогда происходит так называемый «тро́ллинг» или травля (размещение в Интернете на форумах, в дискуссионных группах, в вики-проектах провокационных сообщений с целью собственного развлечения и созданием конфликтов между участниками). Это необходимо

для установления круга знакомых, учителей и родителей подростка с целью направления им полученных провокационных фотографий, а возможно и с целью шантажа и вымanивания определенной денежной суммы.

Ст. 20.3.1. КоАП РФ. Действия, направленные на возбуждение ненависти либо вражды, а также на унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, совершенные публично, в том числе с использованием информационно-телекоммуникационных сетей, включая сеть "Интернет", если эти действия не содержат уголовно наказуемого деяния, - влекут наложение административного штрафа на граждан в размере от десяти тысяч до двадцати тысяч рублей, или обязательные работы на срок до ста часов, или административный арест на срок до пятнадцати суток.

Рассмотрение органами внутренних дел обращений по указанной тематике находится на особом контроле Прокуратуры РФ. При подтверждении фактов нарушения прав и свобод граждан виновные лица подлежат привлечению к установленной законом ответственности.

Органы внутренних дел могут привлечь к установленной законом ответственности за **пропаганду либо публичное демонстрирование нацистской атрибутики или символики,** либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены (ст.20.3КоАП).

Социальные сети являются одним из способов вовлечения студентов в шантаж или же запрещенные РФ группы, подталкивающие молодых людей к совершению каких-либо противозаконных действий (насилие, жестокость). Социальные сети активно используются злоумышленниками для вовлечения детей и подростков в распространение порнографических материалов с участием несовершеннолетних посредством сети Интернет. В ходе электронного общения создаются условия, побуждающие подростка направить свои откровенные фотографии. После их получения данные изображения распространяются на тематических форумах, файлообменных системах и фото и видеопорталах.

Интернет-знакомства.

Мошенники с сайтов знакомств – это особый тип людей, способный втираться в доверие к людям, очаровывать их с целью завладеть деньгами, имуществом. Им свойственно обычно глубокое знание психологии, умение построить общение так, что жертвы сами, добровольно отдают им

материальные ценности. Причем в такую ловушку могут попасть как девушки, так и юноши.

Также нужно помнить, что законодательством предусмотрено большое количество запрещенной информации, размещать которую нельзя ни на своих, ни на чужих страницах в сети Интернет. Это материалы о распространении наркотиков и детской порнографии, материалы о суициде, призывы к массовым беспорядкам.

В заключение хотелось бы еще раз предостеречь всех пользователей социальных сетей: интернет – это находка для преступников. Поэтому в целях безопасности не стоит размещать в открытом доступе свои личные данные: номера телефонов; домашний адрес; реквизиты своих документов; номера банковских карт и счетов и т.п. А также помните: в социальных сетях нередки взломы аккаунтов мошенниками, которые после взлома производят рассылки друзьям и контактам пользователя (например, просят перевести им деньги). Поэтому будьте внимательны в общении. Соблюдайте несложные правила, о которых мы с вами сегодня поговорили и вы сможете сделать свое общение в социальных сетях безопасным и избежать целого ряда возможных проблем.

3. Проведение викторины «Безопасное общение в сети Интернет».

Правила викторины:

1. Обучающиеся делятся на 2 группы, выбирают капитана и название команды.

2. Ведущий задает вопрос. Время для обсуждения вопроса - 1 мин.

3. После обсуждения вопроса команда, которая быстрее поднимет руку, будет отвечать первой.

4. Отвечать должен только капитан команды.

5. Если команда не может ответить на вопрос, то право ответа переходит их соперникам.

6. За правильный ответ команда получает 1 балл.

7. Побеждает команда, набравшая большее количество баллов.

Вопросы викторины «Безопасное общение в сети Интернет».

1. Ты зашёл на незнакомый сайт. Вдруг на экране компьютера появились непонятные тебе сообщения. Что ты сделаешь?

1) Быстро закроешь сайт.

2) Обратишься к родителям за помощью.

3) Сам устранишь неисправность.

Правильный ответ: Всегда спрашивай родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.

2. На адрес твоей электронной почты пришло сообщение: файл с игрой от неизвестного тебе пользователя. Как ты поступишь?

1) Скачаешь файл и начнешь играть.

2) Не будешь открывать файл.

3) Отправишь файл своим друзьям.

Правильный ответ: Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Убедись, что на твоем компьютере установлено антивирусное программное обеспечение. Научись его правильно использовать. Помни о том, что эти программы должны своевременно обновляться.

3. Ты захотел скачать картинку в Интернете, нажал кнопку «скачать», на экране появилось сообщение с просьбой отправить SMS на указанный номер. Как тебе поступить?

1)Отправить SMS на указанный номер.

2)Проверить этот номер в Интернете.

3)Не скачивать больше картинки.

Правильный ответ: Если хочешь скачать картинку или мелодию, но тебя просят отправить смс — не спеши! Сначала проверь этот номер в интернете — безопасно ли отправлять на него смс и не обманут ли тебя. Сделать это можно на специальном сайте.

4. Ты познакомился в Интернете с учеником, которого ни разу не видел. Однажды он приглашает тебя встретиться с тобой в парке. Что ты будешь делать?

1)Пойдешь на встречу.

2)Пойдешь на встречу вместе с мамой или папой.

3)Не пойдешь на встречу.

Правильный ответ: Не встречайся офлайн без родителей с людьми из Интернета. В сети Интернет многие люди рассказывают о себе неправду.

5. Новый друг, с которым ты познакомился вчера в Интернете, попросил тебя срочно сообщить ему такую информацию: номер телефона, домашний адрес, кем работают родители. Как ты поступишь?

1)Сообщишь ему нужные сведения.

2)Не сообщишь через Интернет, а сообщишь при встрече.

3)Посоветуешься с родителями.

Правильный ответ: Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!

6. Ты решил опубликовать в Интернете свою фотографию и фотографии своих одноклассников. Можно ли это сделать?

1)Нет, нельзя.

2)Можно, с согласия одноклассников.

3)Можно, согласие одноклассников не обязательно.

Правильный ответ: Ст. 152.1 Гражданского кодекса (ГК) РФ устанавливает, что любое публичное использование изображений физических лиц, включая размещение в социальных сетях, должно происходить только с согласия таких лиц.

7. Тебе купили компьютер. Теперь целый день ты проводишь за компьютером. Через несколько дней у тебя стали слезиться глаза, появились боли в руках. Что делать?

1)Продолжать проводить время за компьютером.

2)Соблюдать правила работы на компьютере.

3)Больше никогда не работать на компьютере.

Правильный ответ: Соблюдать правила работы на компьютере: Расстояние от глаз до экрана компьютера должно быть не менее 50 см. Продолжительность одного занятия – не более 60 минут. После 10–15 минут непрерывных занятий за ПК необходимо сделать перерыв для проведения физкультминутки и гимнастики для глаз. Продолжительное сидение за компьютером может привести к перенапряжению нервной системы, нарушению сна, ухудшению самочувствия, утомлению глаз.

8. У тебя появилось много друзей в Интернете. Вдруг стали приходить сообщения с неприятным, грубым содержанием. Что ты должен сделать?

1)Оскорбить обидчика.

2)Не отвечать обидчику тем же, а продолжить с ним общение.

3)Сообщить взрослым об этом.

Правильный ответ: Сообщить взрослым о сообщениях с неприятным, грубым содержанием.

9. На адрес твоей электронной почты стали часто приходить письма, многие из которых называются “спам”. Что это за письма?

1)Обычные письма, их можно открывать и читать.

2)Письма, в которых находится важная информация.

3)Письма, которые нельзя открывать и читать.

Правильный ответ: Не открывайте спам. Если же вы открыли письмо и поняли, что это спам, сразу же закройте его. Ни в коем случае не нажимайте на ссылки или кнопки, не загружайте вложенные файлы из сообщений от подозрительных отправителей — в них могут содержаться вредоносные программы, которые крадут ваши личные данные и подвергают угрозе ваш компьютер.

10. Какое слово зашифровано ниже?

Е Б П А Н С Т Ь З О О С

Правильный ответ: безопасность.

11. Т Е Р О М П Ь Ю К

Правильный ответ: компьютер.

12. Какие сайты лишние?

1) Образовательные сайты.

2) Официальные сайты поиска работы в вашем городе.

3) Сайты с рекламой табака и алкоголя.

4) Сайты, посвященные морфологическим словарям и проверке правописания. Правильный ответ. Сайты с рекламой табака и алкоголя.

4. Заключительное слово преподавателя, подведения итогов, оценки.

Ребята, сегодня мы с вами узнали Правила общения в сети Интернет, а так же какая юридическая ответственность за их нарушения предусмотрена законами РФ. Надеемся, что вы будете соблюдать эти правила. А для того, чтобы вы получше запомнили и соблюдали правила общения в сети Интернет, мы дарим вам по буклету, в котором содержится основная

информация по рассмотренной нами теме. Желаем, чтобы сеть Интернет приносила вам только пользу.

Кроме того, сегодня вы участвовали в мероприятии в стенах ГБПОУ Республики Марий Эл «Йошкар-Олинский строительный техникум». Студенты здесь получают образование по юридическим специальностям «Правоохранительная деятельность» и «Право и организация социального обеспечения». Надеемся, мы заинтересовали вас юридическими знаниями. Будем рады видеть вас в качестве абитуриентов ГБПОУ Республики Марий Эл «Йошкар-Олинский строительный техникум».

Успехов вам!