Министерство образования, науки и молодежной политики
Краснодарского края
Государственное бюджетное профессиональное образовательное
учреждение Краснодарского края
«КРАСНОДАРСКИЙ ТОРГОВО-ЭКОНОМИЧЕСКИЙ КОЛЛЕДЖ»

Ширвари О. Е.

Тематическое мероприятие

«Интернет – территория безопасности»

Сценарий

г. Краснодар 2021г.

Составитель- Ширвари О.Е., преподаватель иностранного языка, ГБПОУ КК «КТЭК».

Сценарий тематического мероприятия, включает в себя правила ответственного и безопасного поведения в современной информационной среде, способы защиты от противоправных посягательств в сети Интернет.
Сценарий предназначен для классных руководителей, планирующих проведение мероприятий о правилах безопасности в сети Интернет.

Утвержден на заседании цикловой методической комиссии «Воспитание»
Протокол № 2 от 23.09 2021г.

Председатель ЦМК_____Е. А. Фоменко

Цели и задачи мероприятия

Цель: обратить внимание обучающихся на возможные угрозы в сети Интернет, повысить грамотность в вопросах безопасности в сети, сформировать общепринятые нормы поведения в сети.

Задачи:

1. Познакомить обучающихся с потенциальными угрозами, которые могут встретиться в сети Интернет.
2. Выработать правила безопасного поведения в сети.
3. Выработать необходимость использования в сети общепринятых нравственных норм поведения.

Как узнать про все на свете?

Ну конечно, в ИНТЕРНЕТЕ!

Там музеи, книги, игры,

Музыка, живые тигры!

Можно все, друзья, найти

В этой сказочной сети!

История интернета

К созданию Интернета человечество шло долгие годы, изобретая новые и новые средства связи: изобретение телеграфа (1836); первый атлантический кабель для связи между континентами (1858); изобретение телефона (1876).

Первый электронный компьютер был создан в Америке в 1946 году и назывался ЭНИАК. Тогда у компьютера не было ни монитора, ни мышки, ни клавиатуры. Он напоминал огромный шкаф. Весил первый компьютер 27 тонн – как 5 взрослых слонов. Память у него была совсем маленькая и вмещала всего 20 цифр.

Днём появления сети Интернет принято считать 29 октября 1969 года. В 9 вечера, между первыми узлами сети, находящимися друг от друга на расстоянии 640 километров – в Калифорнийском университете Лос-Анджелеса и в Стэндфордском исследовательском институте – провели первый сеанс связи. Оператор Чарли Клайн пытался выполнить удалённое подключение к компьютеру, находящемуся в Стэнфорде. Успешную передачу каждого введённого символа его коллега Билл Дювалль подтверждал по телефону. Вначале удалось отправить всего три символа «LOG», после чего сеть перестала работать. Символы «LOG» должны были быть словом LOGON (команда входа в систему). В рабочее состояние систему вернули уже к половине одиннадцатого вечера, и следующая попытка оказалась успешной.

После первой успешной передачи данных в сети ARPANET следующим значимым этапом стала разработка в 1971 году первой программы для отправки электронной почты по сети. Данная программа мгновенно обрела популярность.

К 1973 году в состав сети были включены первые зарубежные организации из Великобритании и Норвегии через трансатлантический телефонный кабель. С этого момента сеть стала считаться международной.

В 70-х годах прошлого века основным предназначением сети была пересылка электронной почты. В то же время появляются первые почтовые рассылки, различные доски объявлений и новостные группы. Бурное развитие различных протоколов передачи данных решили данную проблему. 1 января 1983 года сеть ARPANET закрепила за собой термин «Интернет».

Следующим этапом развития была разработка системы доменных имён (англ. Domain Name System, DNS), которая состоялась в 1984 году.

Так же в этом году появляется серьёзный конкурент сети ARPANET – межуниверситетская сеть NSFNet (англ. National Science Foundation Network).

В 1989 году знаменитый британский учёный Тим Бернерс-Ли предложил концепцию Всемирной паутины.

В 1990 году сеть ARPANET, проиграв в конкурентной борьбе NSFNet, прекратила своё существование. Так же в этом году состоялось первое подключение к сети Интернет по телефонной линии (Dialup access – «дозвон»).

1991 год ознаменовался общедоступностью Всемирной паутины в Интернете.

1990-е годы произошло массовое объединение большинства существовавших сетей под флагом Интернет. Открытость технических стандартов во много способствовала быстрому росту сети. К 1997 году в Интернете насчитывалось около 10 млн компьютеров и более 1 млн доменных имён. Сегодня Интернет – популярнейшее средство для обмена информацией.

Сейчас получить доступ в интернет можно через телефон, радио-каналы, сотовую связь, спутники связи, кабельное телевидение, специальные оптико-волоконные линии и даже электропровода. А 22 января 2010 года прямой доступ в Интернет появился и на Международной космической станции.

Сеть интернет связывает миллионы компьютеров по всему миру и уже проникла во все сферы человеческой жизни. Число пользователей интернета стремительно растет, особенно увеличивается состав юной аудитории.

В современном мире Интернет превратился в важнейший канал информации, стал неотъемлемой частью современной цивилизации. Вряд ли можно теперь представить человеческое общение, работу СМИ, образование, политическую жизнь, научные исследования и развлечения без интернет-технологий. Интер-

нет стал средой, влияющей на жизнь многих миллионов пользователей, как взрослых, так и детей.

Сегодня формирование личности детей, их установок, мотивов, ценностных ориентиров и поведенческих навыков происходит на стыке виртуального мира и реальности. Ребята «живут» в мире интернета и цифровых технологий: оформляя страницы и общаясь в блогах, социальных сетях, обмениваясь информацией через сервисы мгновенных сообщений и электронные энциклопедии, участвуя в сетевых играх и сообществах игроков.

Развитие глобальной сети изменило привычный образ жизни, расширило границы знаний и опыта. Теперь появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всём мире.

Всемирная сеть содержит намного больший объем сведений, чем самые крупные библиотеки в мире: в интернете доступны справочные материалы, исторические документы, классическая литература и многое другое.

Интернет дает пользователю огромные возможности как высокотехнологичный источник коммуникации, как инструмент поиска и получения информации. Для того чтобы эффективно использовать этот инструмент, нужны как умения обращаться с ним, так и определенный жизненный опыт, позволяющий не захлебнуться в океане неограниченных возможностей интернета, вовремя разглядеть подводные камни, рифы и водовороты виртуального пространства.

Опасности в Интернете

Существует множество рисков, которые делают наше пребывание в Интернете не таким уж безопасным. Остановимся на них подробнее.

Вредоносные программы

Вредоносные программы — это разнообразное программное обеспечение, умышленно созданное для нанесения вреда электронным устройствам или похищения информационных ресурсов, данных. Это вирусы, «троянские кони», «черви», «боты», программы слежки. Вредоносные программы, попадая на компьютер, способствуют снижению скорости при обмене данными, а также используют наш компьютер как базу для распространения своих вредоносных данных. Они могут использовать наш e-mail или профиль социальной сети как разносчика спама. Такие опасные файлы могут попадать на наши компьютеры:

- посредством посещения сомнительных веб-сайтов и скачанных с них файлов;

- из электронной почты через полученный спам;

- при помощи электронных носителей.

Кибермошенничество

Это один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует вашу личную информацию, что предполагает мошенничество или обман. Четыре из пяти уголовных дел, расследуемых в России в плане киберпреступлений, связаны именно с Интернет-мошенничествами (кибермошенничеством).

К кибермошенничеству относится:

Фишинг - это преступная тактика, используемая интернет-мошенниками с целью обогащения, за счет кражи персональной информации жертвы.

Для фишинга характерны:

- Неожиданные сообщения в мессенджерах, смс, соцсетях и электронной почте от имени авторитетной организации (например, банка, платежной системы, онлайн-магазина и т.д.) с побуждением, будь то угроза или просьба, перейти по фишинговой ссылке, либо ввести информацию в прикрепленную к письму форму.

- Зловредные баннеры и всплывающие окна, ведущие на фишинговые страницы.

Помимо классического фишинга существуют и другие способы выманивания денежных средств у доверчивых интернет-пользователей. Среди таковых:

Вишинг – вид телефонного мошенничества, когда злоумышленники звонят и под видом сотрудника банка, финансовой организации и проч. выманивают у жертв реквизиты банковской карты или побуждают совершить какие-либо действия с банковским счетом.

Смишинг - вид фишинга через смс.

Множество объявлений в социальных сетях, использующих призывы к благотворительности и давящие на жалость.

Социальные сети

Несмотря на то, что социальные сети были созданы с благими намерениями, назвать их безопасным местом для общения нельзя: там слишком большой по-

ток ненужной информации — от имеющей возрастные ограничения до запрещенной.

Регистрируясь в той или иной соцсети, человек принимает условия её пользовательского соглашения. В соответствующем разделе указывается, какого возраста должен достичь владелец аккаунта. Например, у таких ресурсов, как Facebook и Instagram, он составляет не менее 13 лет. Однако в действительности дети часто указывают вымышленный год рождения и успешно регистрируются на этих сайтах и в 7–10 лет и даже раньше.

Регистрируясь в социальной сети, следует понимать, что действия на своей страничке могут просматриваться различными пользователями.

Доступная информация является уязвимой. Каким образом? Например, появлением кибербуллинга или груминга.

Кибербуллинг представляет собой появление сообщений в социальных сетях, содержащих угрозы, оскорбления, запугивание или травлю. Есть случаи, когда чью-то страницу могут взломать, разместив на ней негативный контент, унижающий и оскорбляющий человека.

Кибербуллинг опасен тем, что агрессор может сохранять анонимность, вовлекать в травлю других людей. Это значит, что шансы поймать агрессора снижаются, но у него появляется возможность оскорбить жертву, распространить недостоверные сведения о ней среди большой группы людей. Кибербуллинг может навредить психологическому и эмоциональному состоянию человека.

Порой травля в сети переходит в реальную жизнь, особенно если агрессор и жертва учатся в одной школе, живут в одном районе.

Вероятность встреч с незнакомыми людьми и **грумминг** — ещё одна опасность использования социальных сетей. Добавляя в друзья совершенно незнакомых людей и общаясь с ними, дети подвергают себя опасности. Нередки случаи, когда, представляясь сверстником в онлайн-чате, злоумышленник настаивает на личной встрече, которая может обернуться насилием или даже похищением.

Контентные риски

Это присутствие в интернете материалов противозаконного, неэтичного и иного вредоносного характера. Такие материалы могут быть представлены текстами, изображениями, звуковыми и видеофайлами, ссылками и баннерами на посторонние сайты. Несовершеннолетний гражданин может столкнуться с порнографическим контентом, призывами к использованию и приобретению нарко-

тиков, призывами к участию в экстремистских действиях. Такой контент может нанести психологический вред сознанию детей и подростков, изменить их ценностные ориентации.

Правила безопасности в интернете

Мы хотим, чтоб Интернет

Был вам другом много лет!

Будете знать правила эти –

Смело плавайте в Интернете.

Для того чтобы обезопасить себя, свою семью, своих родителей от опасностей Интернета и причинения возможного ущерба, вы должны предпринимать следующие меры предосторожности при работе в Интернете:

1. Никогда не показывайте личную информацию в Интернете, такую, как адрес, номер телефона, имя, расположение школы, имена родителей. Веб-сайты или другие онлайн-сервисы могут попросить дать информацию для того, чтобы участвовать в конкурсах или получить бесплатные подарки. Некоторые веб-сайты не предоставляют доступ, если пользователь не дает им личной информации. Однако, как только личная информация дана, ваша конфиденциальность может быть нарушена. Имена могут в конечном итоге пойти на продажу в базе данных, или еще хуже, эта информация может быть использована для причинения вреда или эксплуатации.

2. Используйте надежный пароль. Первое и главное правило сохранности Ваших данных, учетных записей, почтовой пересылки это надежный пароль. Периодически меняйте пароли на самых важных сайтах. Так вы уменьшите риск взлома вашего пароля.

3. Всегда информируйте своих родителей, когда сталкиваетесь с чем-нибудь в Интернете, что заставляет чувствовать себя неловко.

4. Никогда, ни при каких обстоятельствах не соглашайтесь встретиться лицом к лицу с виртуальным знакомым с кем переписывались в Интернете без разрешения родителей. Если всё-таки встреча состоится, она должна быть в общественном месте, и родители должны быть в курсе.

5. Никогда не отвечайте на сообщения или объявления, которые являются сексуально непристойными, угрожающими или заставляющими себя чувствовать неловко в любом случае.

6. Никогда не отправляйте личные материалы для онлайн-друзей, такие, как адрес, номер телефона или фотографии, без предварительного информирования родителей.

7. 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.

8. 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.

9. Скачивайте программы с официальных сайтов разработчиков. Не скачивайте программы с подозрительных сайтов или с файлообменников. Так вы уменьшите риск скачать вирус вместо программы.

10. 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.

11. Если вы работаете за компьютером, к которому имеют доступ другие люди, не сохраняйте пароли в браузере. В противном случае любой, кто имеет доступ к этому компьютеру, сможет зайти на сайт, используя ваш пароль.

12. Не открывайте письма от неизвестных вам пользователей (адресов). Или письма с оповещением о выигрыше в лотерее, в которой вы просто не участвовали.

13. Не нажимайте на всплывающие окна, где 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.

14. Уважайте друг друга в социальных сетях. Оскорбляя даже неизвестного вам человека, помните, что вы сделали это и в реальной жизни!

Пользуясь этими правилами безопасности в Интернете, вы существенно уменьшите риск получить вирус на свой компьютер или потерять учетную запись на любимом сайте. Будьте внимательны! Станьте грамотными потребителями цифровой эпохи!