МИНИСТЕРСТВО ОБРАЗОВАНИЯ СТАВРОПОЛЬСКОГО КРАЯ
государственное бюджетное профессиональное образовательное учреждение
«Ставропольский строительный техникум»

ЦИКЛОВАЯ КОМИССИЯ ЕСТЕСТВЕННО-МАТЕМАТИЧЕСКИХ ДИСЦИПЛИН

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ ОТКРЫТОГО МЕРОПРИЯТИЯ

«МЕРОПРИЯТИЕ «**ОСТОРОЖНО МОШЕННИКИ!**» ОБ ИССЛЕДОВАНИИ ПОВЕДЕНИЯ МОШЕННИКОВ В РАЗЛИЧНЫХ СОЦИАЛЬНЫХ СЕТЯХ И СТАТИСТИКЕ ОТКЛИКОВ НА НИХ»

для студентов 1 курсов очной формы обучения всех специальностей

СТАВРОПОЛЬ, 2021

РАССМОТРЕНО
на заседании цикловой комиссии
естественно-математических дисциплин
Протокол №10
«18» мая 2021 г.
Председатель цикловой комиссии
_____ / Н. Б. Берлова /

РЕКОМЕНДОВАНО
Методическим советом
ГБПОУ ССТ
Протокол № 10
«25» мая 2021 г.

СОГЛАСОВАНО
Л. В. Белоусова,
заместитель директора по учебно-
методической работе и качеству
«19» мая 2021 г.
_____

СОГЛАСОВАНО
В. В. Ткаченко,
заместитель директора по ВР
«19» мая 2021 г.
_____

Рецензент:
Л. В. Печалова, кандидат исторических наук
методист Центра менеджмента качества и
методической работы техникума
«18» мая 2021 г.
_____

Разработчики:
Абрамова Л. А., преподаватель общеобразовательных дисциплин
_____ / Л. А. Абрамова /

Данилова М. И., преподаватель общеобразовательных дисциплин
_____ / М. И. Данилова /

«17» мая 2021 г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Современное общество принято называть информационным, поэтому каждый человек должен обладать такими качествами, которые позволили бы ему быть успешным в IT насыщенной среде, то есть обладать высоким уровнем информационной культуры. Одной из составляющих информационной культуры человека является умение извлекать информацию из различных источников, в том числе и из Интернет-ресурсов, не нарушая свою информационную безопасность.

Интернет – уникальная реальность нашего с вами времени. Это безграничный мир информации, где есть не только развлекательные и игровые порталы, но и много полезной информации для учёбы. Здесь можно общаться со своими друзьями в режиме онлайн, можно найти новых друзей, вступать в сообщества по интересам. Информация, оперативно обеспечивающая ваши ежедневные потребности, – все это Интернет.

Почему же мы вынуждены предупреждать об опасностях виртуального мира, если в нём так много всего хорошего и полезного? Достаточно большая часть интернет-пользователей ищет не друзей в Интернете, а свои жертвы. Дело в том, что недобросовестные граждане – мошенники, наркодилеры, иные злоумышленники, асоциальные и психически нездоровые люди по-своему оценили возможности Интернета.

Ведь именно Всемирная паутина дает возможность преступникам действовать анонимно. Поэтому небезопасное поведение в сети Интернет может нанести вред и вам, и вашим родным и близким людям.

Обезопасить себя не так уж и трудно – достаточно серьезно отнестись к проблеме кибербезопасности и соблюдать простые правила, о которых мы расскажем.

Мы поговорим о направлениях по обеспечению кибербезопасности:

– видах мошенничества в сети Интернет;

– мошенничество, связанное с блокированием программного обеспечения компьютеров пользователей сети интернет;

– виртуальное или кибермошенничество;

– нарушение морали и этики в онлайн-общении, троллинг, разрушающий ваше личное пространство.

Место проведения: ГБПОУ ССТ, актовый зал.

«МЕРОПРИЯТИЕ «ОСТОРОЖНО МОШЕННИКИ!» ОБ ИССЛЕДОВАНИИ ПОВЕДЕНИЯ МОШЕННИКОВ В РАЗЛИЧНЫХ СОЦИАЛЬНЫХ СЕТЯХ И СТАТИСТИКЕ ОТКЛИКОВ НА НИХ»

Форма проведения: лекционная.

Время проведения: 60 минут.

Методическая цель: обратить внимание обучающихся на возможные угрозы в сети Интернет, повысить грамотность обучающихся в вопросах безопасности в сети, формировать общепринятые нормы поведения в сети.

Цели:

Образовательные: создать условия для формирования у обучающихся навыков информационной культуры и умений делать обобщения на основе полученных данных и входящей информации.

Развивающие: способствовать развитию познавательного интереса, творческой активности обучающихся, развитию воли и стремления к достижению положительного результата; создать условия для формирования приёмов логического мышления, информационной культуры, развивать способность анализировать и обобщать, делать выводы; расширять кругозор обучающихся.

Воспитательные: способствовать воспитанию информационной культуры, умению индивидуально искать пути решения поставленной задачи, предотвратить или снизить риски кибератак, исключить утечки или повреждение данных, а также минимизировать сбои в работе систем.

Задачи:

– ознакомить обучающихся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет.

– выработать правила безопасного поведения в сети.

– выработать необходимость использования в сети общепринятых нравственных норм поведения.

Ожидаемые результаты:

– повышение уровня осведомленности обучающихся о проблемах безопасности при использовании сети Интернет, потенциальных рисках при использовании Интернета, путях защиты от сетевых угроз.

– формирование культуры ответственного, этичного и безопасного использования Интернета.

А так же обеспечивает достижение студентами следующих результатов:

личностных (ЛР):

ЛР 3 умение использовать достижения современной информатики для повышения собственного интеллектуального развития в выбранной профессиональной деятельности, самостоятельно формировать новые для себя знания в профессиональной области, используя для этого доступные источники информации;

ЛР 4 умение выстраивать конструктивные взаимоотношения в командной работе по решению общих задач, в том числе с использованием современных средств сетевых коммуникаций;

ЛР 5 умение управлять своей познавательной деятельностью, проводить самооценку уровня собственного интеллектуального развития, в том числе с использованием современных электронных образовательных ресурсов;

ЛР 6 умение выбирать грамотное поведение при использовании разнообразных средств информационно-коммуникационных технологий, как в профессиональной деятельности, так и в быту.

метапредметных (МПР):

МПР 1 использование различных видов познавательной деятельности для решения информационных задач, применение основных методов познания (наблюдения, описания, измерения, эксперимента) для организации внеурочной деятельности с использованием информационно-коммуникационных технологий;

МПР 2 умение анализировать и представлять информацию, данную в электронных форматах на компьютере в различных видах;

МПР 3 умение использовать средства информационно-коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;

МПР 4 умение вести дискуссии, доступно и гармонично сочетая содержание и формы представляемой информации средствами информационных и коммуникационных технологий.

Воспитательный потенциал мероприятия направлен на достижение следующих личностных результатов, составляющих Портрет выпускника СПО, определенного рабочей Программой воспитания:

ЛР 4 Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионально конструктивного «цифрового следа».

ЛР 7 Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 10 Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

Оборудование: персональные компьютеры с выходом в сеть Интернет, проектор, микрофон.

Внеурочное мероприятие проходит в один этап.

1. Введение. Вступительное слово преподавателя
2. Основная часть

1. Проведение мероприятия

План:

1. Организационный момент, представление выступающих (1-2 минуты).
2. Классификация опасностей в сети интернет (до 10 минут)
3. 20 шокирующих фактов о социальных сетях Статистика экономических преступлений в сети интернет. Психологическая защита в сети интернет от экономических преступлений (до 20 минут)
4. Техническая защита в сети интернет (до 10 минут).
5. Подведение итогов (3 минуты).

Ход мероприятия

Вступительное слово ведущего:

Здравствуйте! Мы живем в век информационных технологий, достаточно много времени проводим в сети в поисках информации, готовясь к занятиям, или просто отдыхая. Мы общаемся с друзьями, участвуем в дискуссиях, обсуждаем новости, оставляем комментарии, выкладываем фотографии. Очень важно научиться правильно вести себя в сети Интернет, знать правила безопасности и этичного поведения. Сегодня мы с вами об этом и поговорим.

Виртуальная реальность, как и любое пространство, несомненно, обладает и достоинствами и недостатками. Существование кибер-опасностей так же неоспоримо, как польза и удовольствие от использования Интернет-ресурсов. За безопасностью пользователей следят государственные структуры, а также и сотрудники Интернет сервисов, администраторы сайтов, модераторы. Однако ежедневно появляются новые жертвы, пострадавшие чаще всего из-за отсутствия грамотности в вопросах безопасности.

Классификация опасностей в сети интернет. **(Сообщение выступающего)**

Проблема интернет-зависимости выявилась с возрастанием популярности сети Интернет. Некоторые люди стали настолько увлекаться виртуальным пространством, что начали предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Резкий отказ от Интернета вызывает у таких людей тревогу и эмоциональное возбуждение. Психиатры усматривают схожесть такой зависимости с чрезмерным увлечением азартными играми. Официально медицина пока не признала интернет-зависимость психическим расстройством, и многие эксперты в области психиатрии вообще сомневаются в существовании интернет-зависимости или отрицают вред от этого явления.

По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. Российские психиатры считают, что сейчас в нашей стране таковых 4—6%. Несмотря на отсутствие официального признания проблемы, интернет-зависимость уже принимается в расчёт во многих странах мира.

Интернет – это не только пространство для поиска информации, ведения личной переписки, знакомства с новыми людьми и общения, это еще и источник опасности, которую можно предотвратить.

Подростки и молодые люди в возрасте 14-25 лет являются наиболее уязвимой группой и подвергаются наибольшей опасности. Они стремятся исследовать свою сексуальность, уйти из-под контроля родителей и завязать новые отношения вне семьи. Несмотря на то, что общение в Интернете может быть полностью анонимным, они больше подвержены опасности, даже если до конца не осознают возможные последствия.

Проблема безопасности личных данных в социальных сетях описана на многих ресурсах, но эта тема сегодня все равно остается актуальной. Полностью обезопасить себя в Интернете, означает полностью от него отказаться, что не является возможным, для современного человека. Любое действие в Интернете несет опасность для пользователя, что может привести к шантажу, потери финансовых средств, потери важных данных.

Социальные сети не являются каким-то сверхбезопасным ресурсом для выставления личной информации. Хотя мы и представить не можем регистрацию в социальной сети без указания города/страны проживания и личных фотографий, не говоря уже о номере телефона, месте учебы, работы и социального статуса в частности. Эта информация может быть использована против Вас, и никто от этого не защищен.

Нужно четко понимать о методах манипулирования в сети интернет, с помощью которых воздействуют мошенники на пользователей. **(Сообщение выступающего)**

А между тем, вопрос об информационной безопасности в социальных сетях является достаточно актуальным. Конечно, люди стараются не афишировать проблемы, с которыми они столкнулись благодаря своей причастности к интернет-сообществам, но 51% опрошенных признались, что их страницу в социальных сетях «взламывали». А вот из мер безопасности опрошенные указывают в основном «сильные» пароли (75 %) использование антивирусных программ, но не подозревают, что этого не достаточно.

(Сообщение выступающего) Социальные сети, такие как Одноклассники, Вконтакте, MySpace, Facebook, Twitter и многие другие позволяют людям общаться друг с другом и обмениваться различными данными, например, фотографиями, видео и сообщениями. По мере роста популярности таких сайтов растут и риски, связанные с их использованием. Хакеры, спамеры, разработчики вирусов, похитители личных данных и другие мошенники не дремлют. Пожалуй, очень стоит прислушаться к советам специалистов компании Microsoft, которые помогут вам защитить ваши персональные данные при работе с социальными сетями [10]:

Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях от других пользователей или друзей. Не следует бездумно открывать все ссылки подряд - сначала необходимо убедиться в том, что присланная вам ссылка ведет на безопасный или знакомый вам ресурс.

• **Контролируйте информацию о себе, которую вы размещаете.** Обычно злоумышленники взламывают учетные записи на сайтах следующим образом: они нажимают на ссылку "Забыли пароль?" на странице входа в учетную запись. При этом для восстановления или установки нового пароля, система может предлагать ответить на секретный вопрос. Это может быть дата вашего рождения, родной город, девичья фамилия матери и т.п. Ответы на подобные вопросы можно легко найти в сведениях, которые вы опубликовали на своей странице в какой-либо популярной социальной сети. Поэтому при установке секретных вопросов необходимо придумывать их самостоятельно (если сайт, на котором вы регистрируетесь, это позволяет) или старайтесь не использовать личные сведения, которые легко найти в сети.

• **Не думайте, что сообщение, которое вы получили, было отправлено тем, кого вы знаете, только потому, что так написано.** Помните, что хакеры могут взламывать учетные записи и рассылать электронные сообщения, которые будут выглядеть так, как будто они были отправлены вашими друзьями. Если у вас возникло такое подозрение, будет лучше связаться с отправителем альтернативным способом, например, по телефону, чтобы убедиться в том, что именно этот человек отправил вам данное сообщение. Точно также необходимо относиться и к приглашениям зарегистрироваться в той или иной социальной сети.

• **Чтобы не раскрыть адреса электронной почты своих друзей, не разрешайте социальным сетям сканировать адресную книгу вашего ящика электронной почты.** При подключении к новой социальной сети вы можете получить предложение ввести адрес электронной почты и пароль, чтобы узнать, есть ли в этой сети пользователи, с которыми вы уже поддерживаете отношения при помощи электронной переписки. Используя эти данные, сайт может рассылать электронные сообщения (например, приглашения присоединиться к этой сети от вашего лица) всем пользователям из вашего списка контактов. Социальные сети должны указывать то, что эти адреса электронной почты будут использованы для этой данной, но зачастую не делают этого.

• **Вводите адрес социальной сети непосредственно в адресной строке браузера или используйте закладки.** Нажав на ссылку, которую вы получили в электронном сообщении или нашли на каком-либо сайте, вы можете попасть на поддельный сайт, где оставленные вами личные сведения будут украдены мошенниками.

• **Не добавляйте в друзья в социальных сетях всех подряд.** Мошенники могут создавать фальшивые профили, чтобы получить от вас информацию, которая доступна только вашим друзьям.

• **Не регистрируйтесь во всех социальных сетях без разбора.** Оцените сайт, который вы планируете использовать, и убедитесь, что вы правильно понимаете его политику конфиденциальности. Узнайте, существует ли на сайте контроль контента, который публикуется его пользователями. К сайтам, на которых вы оставляете свои персональные данные, необходимо относиться с той

же серьезностью, которой требуют сайты, где вы совершаете какие-либо покупки при помощи кредитной карты.

• **Учитывайте тот факт, что все данные, опубликованные вами в социальной сети, могут быть кем-то сохранены.** На большинстве сервисов вы можете в любой момент удалить свою учетную запись, но, не смотря на это, не забывайте, что практически любой пользователь может распечатать или сохранить на своем компьютере фотографии, видео, контактные данные и другие оставленные вами сведения.

• **Проявляйте осторожность при установке приложений или дополнений для социальных сетей.** Многие социальные сети позволяют загружать сторонние приложения, которые расширяют возможности личной страницы. Довольно часто такие приложения используются для кражи личных данных, поэтому к их использованию необходимо относиться также серьёзно, как и к установке на свой компьютер программ, которые вы можете найти в Интернете.

• **Старайтесь не посещать социальные сети с рабочего места.** Любая социальная сеть может стать средой для распространения вирусов и других вредоносных или шпионских программ, что может привести не только к заражению вашего компьютера и всей корпоративной сети, но и к потере данных, составляющих коммерческую тайну вашей компании.

Итак, выше приведенные правила, пожалуй, совпадают не только с мнением ведущих специалистов, но и абсолютно не противоречат простой человеческой логике. Так давайте соблюдать эти простые правила и будем немножечко увереннее в своей информационной безопасности!

Список используемой литературы

1. **Виленская, Г. А.** Исследования психологии интернета в «Психологическом журнале»: некоторые итоги и перспективы / Г. А. Виленская // Психологический журнал. – 2019. 40(4), – С. 5–14.

2. **Войскунский, А. Е.** Перспективы становления психологии Интернета / А. Е. **Войскунский** // Психологический журнал. – 2013. 34(3), С. – 110–118.

3. **Войскунский, А. Е.** Психология в сетевом контексте: начальный период. В Информационное общество: образование, наука, культура и технологии будущего/ А. Е. Войскунский // Сборник научных статей.– Санкт-Петербург : Издательство Университет ИТМО. – 2018. Выпуск 2, – С. 268–279 (Труды XXI Международной объединенной конференции «Интернет и современное общество, 30 мая-2 июня 2018 г).

4. **Гаврилов М. В.** Информатика и информационные технологии : учебник для среднего профессионального образования / М. В. Гаврилов, В. А. Климов. - 4-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2019. – 383 с. – (Профессиональное образование). – ISBN 978-5-534-03051-8. – Текст : электронный // ЭБС Юрайт. – URL: https://urait.ru/bcode/433276 (дата обращения: 29.01.2021).

5. **Златопольский, Д. М.** Занимательная информатика: Научно-популярное / Златопольский Д.М., - 4-е изд., (эл.) – Москва : Лаборатория знаний, 2017. – 427 с.: ISBN 978-5-00101-540-6. – Текст : электронный. – URL: https://znanium.com/catalog/product/977830 (дата обращения: 02.03.2021).

6. **Лукинова, О. В.** Цифровой этикет. Как не бесить друг друга в интернете / О. В. Лукинова. – Москва : Эксмо, 2020. – 240 с. (Этикет без границ. Новые правила для нового времени).

7. **Михеева Е. В.** Информатика [Текст]: учебник для студ. учреждений СПО / Е.В. Михеева, О.И. Титова – М.: ИЦ «Академия», 2018. – 400 с.

8. **Угринович Н. Д.** Информатика : учебник / Угринович Н.Д. – Москва : КноРус, 2021. – 377 с. – ISBN 978-5-406-08167-9. – URL: https://book.ru/book/939221 (дата обращения: 28.02.2021). – Текст : электронный.

9. **Хлебников А. А.** Информатика : учебник для студентов образовательных учреждений среднего профессионального образования / А. А. Хлебников. – Изд. 2-е, испр. и доп. – Ростов-на-Дону : Феникс, 2017. – 446, с. : ил.

10. **Цветкова М. С.** Информатика : учебник для студ. учреждений сред. проф. образования / М. С. Цветкова, И. Ю. Хлобыстова. – 6-е изд., стер. – М. : Издательский центр «Академия», 2020. – 352 с. : ил., [с цв. вкл.]. ISBN 978-5-4468-9008-8. Текст : электронный // ЭБС Издательский центр «Академия». – URL: https://www.academia-moscow.ru/reader/?id=452487 (дата обращения: 03.05.2021).

Приложение

Памятка
Основные правила безопасного поведения в сети «Интернет»

1. Приложите максимум усилий к защите ваших технических устройств:

- регулярно обновляйте операционную систему;
- используйте лицензионную антивирусную программу;
- применяйте файервол;
- создавайте резервные копии важных файлов;
- используйте надёжные пароли;
- периодически меняйте пароли на самых важных для вас сайтах;
- скачивайте программы только с официальных источников;
- не посещайте подозрительные сайты;
- закрывайте сомнительные всплывающие окна;
- не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они ни были.

2. При работе с электронной почтой:

- никогда не открывайте подозрительные сообщения или вложения электрон-ной почты, полученные от незнакомых людей. Вместо этого сразу удалите их, выбрав команду в меню сообщений.
- никогда не отвечайте на спам;
- никогда не пересылайте «письма счастья» и другой подобный спам. Вместо этого сразу удаляйте такие письма.

3. Защите самих себя:

- не вводите личную и конфиденциальную информацию на непроверенных и подозрительных сайтах;
- внимательно относитесь к собеседникам в Интернете, сообщайте важную информацию только проверенным людям;
- при работе за компьютером, к которому имеют доступ другие люди, не сохраняйте пароли в браузере.

4. Соблюдайте правила:

- • помните, что в виртуальном пространстве ответственность наступает по реальным законам;
- • уважительно и добросовестно относитесь к другим пользователям сети Интернет.