Голубева Елена Николаевна, Толстикова Елена Иннокентьевна, преподаватели информатики ГБПОУ НСО «Новосибирский автотранспортный колледж»

**Методическая разработка внеклассного мероприятия**

**«Единый урок безопасности в сети Интернет»**

**Пояснительная записка**

Быстрое развитие информационных технологий, появление огромного количества интернет-магазинов и сервисов, доступность и простота использования облачных и мобильных технологий делают нашу жизнь более комфортной. Однако, за комфортом и простотой часто скрываются и негативные факторы. Например, навязчивые Интернет-ресурсы (СМИ, реклама), содержащие негативный и агрессивный контент, фишинг, вредоносные программы. Таким образом, необходимо повышать информационную культуру обучающихся по безопасной работе в сети Интернет в целях предотвращения негативных последствий массового использования Интернета и их защиты от негативной информации. Поэтому, в соответствии с рекомендациями Минобрнауки России во всех образовательных учреждениях, начиная с 2014 года, проводится Единый урок по безопасности в сети «Интернет»

Сценарий мероприятия предназначен для проведения единого урока для студентов 1 и 2 курса всех специальностей

Цели мероприятия:

* привлечь внимание обучающихся к проблеме информационной безопасности.
* повысить уровень кибербезопасности и цифровой грамотности
* выработать умение осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития с учетом правил безопасной работы в сети Интернет
* показать важность умения работать в коллективе и взятия на себя ответственности за выполненное задание

Оборудование:

* компьютер;
* мультимедийный проектор, экран;
* таблица для учёта баллов;
* презентация с заданиями;
* раздаточный материал для команд;
* секундомер

**Ход урока**

1. Организационный момент

2. Вступительное слово

В эпоху современных информационных технологий каждый из нас постоянно использует компьютеры и мобильные телефоны, и конечно никто не обходится без использования глобальной сети Интернет. Мы используем поисковые системы для поиска различной информации, электронную почту, интернет-магазины, онлайн платежи, социальные сети. У нас есть возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всем мире. Но с другой стороны, кроме положительных моментов есть много негативных факторов, которые скрывает в себе сеть Интернет. Об этом и будет наше занятие

На нашем мероприятии вы посмотрите видеофильм, послушаете доклады, которые помогут вам при выполнении тестового задания, и приумножите свои знания по правилам безопасной работы в сети интернет. А также продемонстрируете свои знания, приняв участие в интеллектуальной игре.

3. Просмотр видеофильма «Безопасная работа в сети интернет».

4. Выступление обучающихся с докладами:

«Как компьютерные технологии влияют на здоровье»

«Мошенники в сети»

«Вирусы»

5. Тест-опрос Безопасность в сети интернет (Приложение 1),

6. Игра «Безопасность в сети интернет

Группа делится на команды (5-7 человек)

Выбирают капитанов и придумывают названия команд, которые заносятся в таблицу для учета баллов, устанавливается очередность ответов командами.

В ходе игры используется презентация (Приложение 2). Баллы, полученные в каждом раунде командой, заносятся в таблицу для учета баллов.

На слайде представлена таблица с номерами вопросов, которые оцениваются от10 до 15 баллов. Капитаны команд по очереди выбирают номер вопроса. Открывается слайд с формулировкой вопроса, а из таблицы соответствующий вопрос удаляется. На размышление команде дается 20 секунд. В случае правильного ответа команда получает соответствующее количество баллов. Если ответ не верен, то команда-соперница может дать ответ и получить баллы для своей команды.

7. Подведение итогов.

Приложение 1

Тест

*Выберите верный ответ:*

1. Ваши друзья жалуются, что с вашего аккаунта во ВКонтакте приходит спам. Ваши действия?
	1. Не буду предпринимать никаких действий
	2. попрошу друзей не переходить по ссылкам, которые приходят от меня, и напишу в техподдержку, сменю пароль от учётной записи во ВКонтакте, от почты, к которой привязан этот аккаунт, и пройдусь по компьютеру антивирусом
	3. сменю пароль от учётной записи ВКонтакте — этого будет достаточно
2. Что безопаснее: работать под учетной записью с ограниченными правами или под учетной записью администратора
	1. С ограниченными правами: злоумышленник не может запустить вредонос или выполнить другие действия без ведома пользователя
	2. С ограниченными правами: у администратора не ограничен доступ к интернету, а значит выше риск подхватить вирус
	3. Как администратор: есть возможность самостоятельно контролировать процессы на компьютере
3. Как известно, злоумышленникам не составляет труда подобрать простой пароль от почты, поэтому рекомендуется подбирать сложные пароли. Какой из этих паролей НЕ является сложным.
	1. 01.02.1998(дата рождения)
	2. PRso18A@(пароль, в котором есть большие и маленькие буквы и специальные символы)
	3. Ghfdbntkm03(пароль, в котором больше восьми символов)
4. Почему не рекомендуется вводить пароли от аккаунтов в публичных wi-fi сетях?
	1. все ответы верны
	2. публичный Wi-Fi более уязвим к атакам злоумышленников, чем, например, домашняя или офисная сеть
	3. публичный Wi-Fi, как правило, не содержит протоколов шифрования или использует устаревшие протоколы, а значит все данные по такой сети будут передаваться в открытом виде
5. Как поступить, если вы получили сообщение в соцсети от друга, который просит денег взаймы?
	1. перевести ему деньги;
	2. переслать сообщение кому-нибудь ещё, кто сможет дать в долг;
	3. проверить друга — спросить, например, как зовут учителя физкультуры в вашей школе
6. Что делать, если вы получили письмо от своего банка, в котором просят сообщить или подтвердить ваши персональные данные?
	1. отправить данные в ответном письме;
	2. сообщить данные по телефону, указанному в письме;
	3. ничего не отправлять, так как банки никогда не запрашивают персональные данные — ни в письмах, ни по телефону.
7. Как распознать поддельный сайт?
	1. по ошибкам в текстах;
	2. по «опечаткам» в адресной строке (например, http://money-yanbex.ru)
	3. по невзрачному дизайну.
8. Своевременное обновление программного обеспечения необходимо для:
	1. эффективной работы
	2. закрытия уязвимостей и исправления критических ошибок в программах.
	3. внесения новых функций и улучшения уже существующих
	4. защиты от мошенничества
	5. все ответы верны
9. Что нужно делать, когда вы заходите в свой аккаунт на компьютере друга?
	1. не нажимать галочку «Запомнить пароль», а также почистить историю после завершения сессии, или включить инкогнито режим браузера
	2. компьютер друга такой же безопасный, как ваш собственный, поэтому можно ничего не предпринимать
	3. попросить друга отвернуться или закрыть глаза, когда вы вводите пароль
10. Установите соответствие между термином и его значением

|  |  |
| --- | --- |
| 1. эксплойт
 | 1. Авторизация с двойной защитой — паролем и одноразовым кодом, который приходит через СМС или генерируется в специальной программе
 |
| 1. двухфакторная аутентификация
 | 1. программа, с помощью которой мошенники через уязвимые места могут получить доступ к управлению системой или к пользовательским данным.
 |
| 1. фишинг
 | 1. метод перебора паролей в котором мошенникам помогают программы-боты. Они просто перебирают символы или, чтобы было быстрее, проверяют пароли по специальным словарям для взломщиков.
 |
| 1. брутфорс
 | 1. — способ обмана, при котором мошенники выдают себя за какой-нибудь известный сервис или организацию. Допустим, присылают письмо от имени банка и попросят у человека пароль от онлайн-кабинета — якобы для решения технических проблем.
 |