Департамент образования администрация г. Перми
Муниципальное бюджетное учреждение
«Центр психолого-педагогической, медицинской и социальной помощи» г. Перми

РАССМОТРЕНО

утверждено на заседании НМС МБУ «ЦППМСП» г. Перми
Протокол № 4 от 29.12.2022г.

СОГЛАСОВАНО

_____О.В. Полторак,
начальник управления воспитания и социализации департамента образования администрации города Перми

УТВЕРЖДАЮ

_____О.А. Митина
и.о. директора МБУ «ЦППМСП» г. Перми

ПРОГРАММА
киберурока «Информационная безопасность»
(для учащихся 11 класса)

г. Пермь, 2022

74. КИБЕРУРОК
«Информационная безопасность» (для 11 класса)

Цель: формирование представления об информационной безопасности.
Задачи:
обучающие:
- познакомить с понятием информационной безопасности
- рассмотреть различные угрозы информационной безопасностиразвивающие:
- совершенствовать коммуникативные навыки через умение излагать мысли, умение вестидиалог
- определить план действий для предотвращения угрозы информационной безопасности

воспитывающие:
- воспитывать ответственность за свои действия

План урока:
1. Организационный момент
2. Подготовка учащихся к усвоению нового материала
3. Теоретическая часть. Изучение нового материала
4. Практическая часть. Первичное закрепление знаний
5. Домашнее задание
6. Итог урока.

Оборудование и методические материалы: Мультимедийный проектор, ПК на РМУ, презентация, набор карточек, памятка для обучающихся.

Ход урока
Организационный момент
Подготовка к усвоению нового материала
Тема урока «Информационная безопасность».
Цель урока: Формирование представления об информационной безопасности.
Теоретическая часть. Изучение нового материала

- Что такое «информационная безопасность»?

Дети высказывают свое мнение, как они понимают этот термин. Обобщая, учитель сообщает определение, которое записывается в тетрадь

Информационная безопасность - это защищенность информации от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации или ее владельцам.

- Какие воздействия могут нанести ущерб информации или владельцу, то есть что представляет угрозу информационной безопасности?

Дети делают свои предположения и определяются 7 направлений:

1. Кража личных данных, утечка информации
2. Вирусы, черви, трояны
3. Спам
4. Хакеры
5. Авторское право, нелицензионное ПО
6. Мошенничество
7. Дезинформация

Задачи информационной безопасности сводятся к минимизации ущерба, а

также к прогнозированию и предотвращению таких воздействий.

Давайте разделимся на группы и установим, какие действия нужно предпринять, чтобы обезопасить себя от таких воздействий.*Работа группами по карточкам, обсуждение - 10 минут, затем представители от каждой группы сообщают всем свои методы защиты (принимая или оспаривая), учитель принимает участие в обсуждении - разрабатывается памятка*

Кража личных данных, утечка информации

- старайтесь не «светить» номер кредитки в Сети;
- совершая онлайновую покупку, обращайте внимание на защищенность канала передачиданных;
- отслеживайте файлы cookies на жестком диске, регулярно проверяйте их принадлежностьи удаляйте подозрительные.

Итог урока

Учитель подводит итог урока, выставляет оценки.

Набор карточек

1 группа Утечка или кража личных данных.

Суть: Ваша персональная информация может оказаться в чужих руках, что грозит печальными последствиями, вплоть до серьезного последствия.

Факты: Если у вас есть кредитная карта и банковский счет, то весьма собланительно выгляди- дит перспектива оплаты услуг Internet-магазинов в режиме on-line. Действительно, это ведьтак удобно! Таким образом, в Европе за прошлый год счета «облегчились» на 533 млн $.

Защита:

2 группа Вирусы.

Суть: На ваш компьютер могут напасть вредоносные программы, уничтожающие данные или приводящие к неработоспособности всего компьютера.

Факты: Вирусов стоит бояться и в оффлайновой жизни, но на просторах Internet распространение вирусов может выливаться в настоящие эпидемии. Коварные создатели вредоносных программ используют почтовые сообщения. Приходится быть осторожными с программами, которые вы скачиваете из Internet.

Защита:

3 группа Спам.

Суть: Ваш почтовый ящик начинает переполняться несанкционированными рекламными сообщениями, делая практически невозможной нормальную обработку электронной почты.Факты: Ленивые и неудачные торговцы, вместо того, чтобы заняться повышением уровня своих товаров и услуг, стремятся делать бизнес на некачественной рекламе.

Защита:

4 группа Хакеры.

Суть: В ваш компьютер могут проникнуть из Internet с целью кражи личной информации либо для использования вашего компьютера в качестве плацдарма для дальнейших атак.

Факты: Всего лишь пару лет можно было успокоить домашних пользователей, что хакерам нужен доступ только на крупные, мощные машины – теперь

времена изменились. Даже информация о подключении к Internet-провайдеру (телефон+логин+пароль) – лакомая добычадля хакера.
Защита:

Приложение 1.

Вирусы, черви, трояны

- приобретите хороший антивирусный пакет, установите его в режиме максимальной без-опасности, и своевременно обновляйте;

Спам

- не сообщайте посторонним ваш адрес электронной почты, особенно тот, который
- предоставлен провайдером или особенно важен для вас;
- пользуйтесь почтовыми серверами с установленными фильтрами.

Хакеры

- никогда не храните пароли на винчестере (даже в зашифрованном виде), не ленитесь каждый раз набирать их вручную;
- отсоединяйтесь от Internet при подозрении на хакерскую атаку, запускайте антивирусную программу, изменяйте пароли;
- старайтесь меньше пользоваться общедоступными программами сомнительного происхождения;
- просматривайте чаще системный реестр на предмет подозрительных записей;
- обязательно делайте резервные копии данных на дискеты или CD R/RW; Авторское право, нелицензионное ПО
- укрепление законодательной базы;
- пресекайте попытки воровства вашего творчества;
- используйте только лицензионное ПО. Мошенничество (денежное надувательство).
- просто будьте более скептичными и менее доверчивыми. Дезинформация.
- разумный скептицизм плюс ее проверка в других средствах массовой информации.

- Рассмотрим, как можно защитить информацию из своего файла от посторонних глаз,защитить файл от изменений.

Демонстрируется презентация.

Создание текстового файла, который требует пароль при открытии

1. Необходимо нажать в строке меню Сервис / Параметры
2. Появится окно Параметры, выбрать вкладку Безопасность
3. В поле Пароль для открытия файла ввести пароль, нажать Ок
4. Появится окно о подтверждении
5. Внимание!!! Не забудьте свой пароль!

Создание текстового файла, который не позволяет вносить изменения

1. Необходимо нажать в строке меню Сервис / Защитить документ
2. Появится справой стороны панель Защита документа
3. В поле Ограничение на редактирование поставить галочку и указать вариант толькочтение
4. Нажать кнопку да, включить защиту.

IV. Практическая часть. Первичное закрепление знаний

Создайте файлы:

• Работа 1, который требует пароль для открытия
• Работа 2, который не позволяет вносить изменения в файл Обучающиеся создают и сохраняют файлы с необходимым условием

V. Домашнее задание

- Выучить записи в тетради. Ознакомить друзей с памяткой.

Приложение 2.

Памятка для обучающихся

БУДЬ БДИТЕЛЕН!

Утечка или кража личных данных.

- *старайтесь не «светить» номер кредитки в Сети;*
- *совершая онлайновую покупку, обращайте внимание на защищенность канала передачи данных;*
- *отслеживайте файлы cookies на жестком диске, регулярно проверяйте их принадлежность и удаляйте подозрительные*

Вирусы.

- *приобретите хороший антивирусный пакет, установите его в режиме максимальной безопасности, и своевременно обновляйте;*

Спам.

- *не сообщайте посторонним ваш адрес электронной почты, особенно тот, который предоставлен провайдером или особенно важен для вас;*
- *пользуйтесь почтовыми серверами с установленными фильтрами.*

Хакеры.

- *никогда не храните пароли на винчестере (даже в зашифрованном виде), не ленитесь каждый раз набирать их вручную;*
- *отсоединяйтесь от Internet при подозрении на хакерскую атаку, запускайте антивирусную программу, изменяйте пароли;*
- *старайтесь меньше пользоваться общедоступными программами сомнительного происхождения;*
- *просматривайте чаще системный реестр на предмет подозрительных записей;*
- *обязательно делайте резервные копии данных на дискеты или CD R/RW.*

Нарушение авторского права.

- *укрепление законодательной базы;*
- *пресекайте попытки воровства вашего творчества.*

Вероятность дезинформации.

- *разумный скептицизм плюс ее проверка в других средствах массовой информации.*

Денежное надувательство.

- *просто будьте более скептичными и менее доверчивыми.*