**Конспект урока**

**Информатика 7 класс**

Учитель Палецкая Алла Юрьевна,

МКОУ Сортавальского МР РК СОШ №1, город Сортавала

**Тема урока: «Создание надежных паролей»**

**Тип урока:**Проект с элементами исследования

**Цель:**организовать проектную деятельность обучающихся на уроке.

**Задачи:**

- образовательные (формирование познавательных УУД):

научить создавать надежные пароли

- воспитательные (формирование коммуникативных и личностных УУД):

умение работать в группе, распределять обязанности при работе в группе, слушать других участников группы

- развивающие (формирование регулятивных УУД)

умение обрабатывать информацию, анализировать и делать выводы; представлять информацию в наглядном виде; оценивать результаты своей работы

**Формы работы учащихся**: парная или в мини-группах

**Организация деятельности учащихся на уроке**:

-самостоятельно выходят на проблему и решают её;

-самостоятельно определяют тему, цели урока;

-работают с данными, анализируют данные

- оформляют результаты в виде таблиц, схем, диаграмм

-делают выводы

-делятся выводами с другими

-оценивают себя и друг друга;

-рефлектируют.

**Необходимое техническое оборудование**: Компьютер учителя, проектор, 7 ноутбуков или стационарных компьютеров, подключенных к локальной сети класса, раздаточный материал (приложения1, приложение 2, приложение 3), электронная презентация, выполненная в программе PowerPoint

**План урока**

1. **Организационный момент. (1мин)**

Здравствуйте. Сегодня на уроке у нас присутствуют гости, давайте их поприветствуем.

Пожалуйста, присаживайтесь.

1. **Целеполагание. (3мин)**

Учитель читает текст или двое обучающихся играют сценку по ролям:

*Миша*: Мой аккаунт в контакте взломали.

*Вася*: И ты из-за этого так расстроен?

*Миша*: Конечно, мои друзья получили ссылку с моей странички и поверили, что это от меня. Там была просьба поддержать в конкурсе и проголосовать. А голосование было платное. Теперь не знаю, как перед ними оправдываться.

*Вася*: У моей знакомой взломали электронную почту и за восстановление данных просили заплатить, а у нее были там важные документы и личная информация. А какой у тебя пароль был?

*Миша*: 15.06.2002 Дата моего рождения. Чтобы не забыть. Она у меня и на страничке в контакте есть. Разве это ненадежный пароль?

Учитель задает вопрос: «С кем из ребят вы согласны и почему?» и просит сформулировать тему урока. Обучающие высказывают свои предположения, и тема урока появляется на слайде: «Как создать надежный пароль».

Учитель задает вопрос: «Как вы думайте, у вас надежные пароли?» По желанию несколько учеников вызываются к учительскому компьютеру и проверяют свой пароль на сайте Microsoft Security.<https://www.microsoft.com/ru-ru/security/pc-security/password-checker.aspx>

 Другие ученики видят результат проверки на экране и убеждаются, что не всегда придуманные ими пароли надежны.

1. **Определение этапов проектной деятельности на уроке**

*На экране слайд*

Процесс разработки проекта с элементами исследования:

1. Определить вопрос или проблему
2. Собрать данные или доказательства
3. Проанализировать данные
4. Сделать выводы
5. Поделиться выводами

Учитель: Давайте создадим исследовательский проект по нашей теме. Мы с вами будем анализировать данные с сайта <http://www.kaspersky.ru//> На каждом этапе работы будем формулировать выводы. Результат проекта оформим в виде презентации. Для того, чтобы вы могли поделиться выводами на каждом этапе работы, воспользуемся возможностями локальной сети класса. Зайдите в папку «общие документы». Найдите там папку «7А». В ней созданы папки с номерами ваших групп. Найдите папку с номером своей группы и внутри создайте документ PowerPoint.

**4.Основные этапы работы**

Задание 1. Оформление титульного листа (5 мин)

Учитель: Каждая презентация начинается с титульного листа. Какая информация обязательно должна быть на титульном листе? Учащиеся отвечают. Задание первое: создайте титульный лист своего проекта, указав название, авторов проекта. Можно добавить элементы оформления.

Задание 2. Какие пароли являются ненадежными (10 минут)

Перед вами документ с аналитической информацией. Прочитайте текст документа и на втором слайде создайте топ 5 самых ненадежных паролей в мире и России (у некоторых групп будет информация о паролях в России, у других групп – в мире. Оформите результат в удобном виде: списком, схемой, диаграммой или таблицей. Устно сделайте вывод. На задание у вас 10 минут.

Проверяем задание 2. Своими выводами делятся ученики двух групп (в мире и России) (3 мин)

Задание 3. Как правильно хранить пароли (7 мин)

 Важно правильно хранить пароль, чтобы он не стал доступен злоумышленникам. Перед вами документ, как люди в России и мире хранят свои пароли. Сравните данные, оформите результат своей работы на слайде. На это задание у вас 7 минут.

Проверяем задание 3. Своими выводами делятся ученики одной группы (3 мин)

Задание 4. Как создать надежный пароль. (7 минут)

Теперь сформулируем 3 основных правила, как создать надежный пароль. Нужно оформить эти правила на слайде. Для этого вы поработайте с текстом.

Проверяем задание 3. Своими выводами делятся ученики одной группы, ученики из других групп высказывают свое мнение, о том, какие 3 правила самые важные (3 мин)

Задание 5 (Практикум по составлению надежного пароля) (3 мин)

Прочитайте алгоритм и выполните задание. Какой пароль у вас получился? Напишите его на слайде.

**Итог урока, рефлексия. (3 мин)**

             Что нового вы узнали сегодня на уроке?   Было ли вам интересно выполнять задания? Напишите свое мнение на листочках, которые лежат перед вами на партах.

**Домашнее задание(3мин)**

Придумайте свой алгоритм создания легкого, но надежного пароля.

**Приложение 1**

**Текст «Самые ненадежные пароли»**

Итак, согласно данным «Лаборатории Касперского» можно выделить 5 самых распространенных паролей во Всемирной паутине. Стоит отметить, что также, согласно опросу аналитического агентства, 45% россиян и 33% пользователей во всем мире отдают предпочтение перечисленным ниже популярным паролям. Злоумышленники же смогут взломать их за считанные секунды, учитывая, что подобную информацию легко найти на страничке соцсети конкретного человека или подобрать комбинацию с помощью специализированных программ.

Дата рождения. Этот наипростейший пароль набрал больше всего голосов опрошенных. 23% россиян и 37% китайцев задают в качестве пароля дату своего рождения. Номер телефона в качестве пароля удерживает второе место как в России (12%), так и в Китае (22%). В Европе лишь 3% пользователей выбирают такой пароль. Кличка домашнего питомца. Если в России кличку любимого животного выбирают только 9%, то в странах Северной Америки – это самый популярный пароль: его используют 15% юзеров. Самые простые сочетания букв и цифр или их последовательность. Подобные пароли не менее распространены, чем клички питомцев, и также не надежны. Различные комбинации 12345, qwerty и другие легко разгадываются злоумышленниками.

Простые слова из русского и английского языка. Один из популярных вариантов – слова пароль или password, «откройся» и разнообразные слова из английского языка.

Источник: [http://www.kaspersky.ru](http://www.kaspersky.ru/)

**Приложение 2**

**Текст «Ненадежные пароли. Мировая статистика»**

Самым популярным паролем в мире, который одновременно остается и самым часто взламываемым, оказался «123456», находясь на этой позиции с 2013 года, а на втором месте — «password» (раньше лидировал в рейтинге). Пароль «12345» резко поднялся на 3-е с 20-ого места, подвинув «12345678» на ступень ниже по сравнению [с прошлым годом](https://hi-tech.mail.ru/news/worst-passwords-2013.html). Тот же, в свою очередь, сместил «qwerty». «123456789» и «1234» заняли шестое и седьмое места в рейтинге соответственно,  а замыкает десятку тройка новичков: «baseball», «dragon», «football».

Примечательно, что «111111», несмотря на кажущуюся простоту, продолжает опускаться и уже находится на 15-ом месте. Это связано, скорее всего, с пониманием пользователей интернета 2014 года о том, что пароль, состоящий из повторяющихся цифр, слишком прост и очевиден, потому и выбирают более сложные вариации: «696969» и «123123» заняли 22 и 23 места соответственно.

**Приложение 2**

**Текст «Где хранят пароли»**

По результатам собственного опроса пользователей Facebook, российские пользователи оказались осмотрительнее остальных в отношении уникальности паролей. Лишь 12% русскоязычных респондентов ответили, что используют один пароль для нескольких учетных записей. В то же время в среднем по миру один и тот же пароль ко всем ресурсам использует каждый пятый пользователь. В США этот показатель еще выше — 23%. Самыми беспечными по результатам опроса оказались мексиканцы — 26% респондентов из Мексики признались, что используют один пароль при авторизации на всех ресурсах. В России бдительность пользователей значительно выше — такую беспечность проявляет лишь каждый десятый.

На безопасность аккаунтов также напрямую влияет способ хранения паролей к ним. Как показало исследование, в этом случае пользователи преимущественно полагаются на свою память: 71% опрошенных в мире хранят пароли в голове, в России этот показатель чуть ниже (53%), но также удерживает лидирующие позиции. Однако существенная часть пользователей поступает не так разумно: 23% опрошенных в мире и 31% россиян записывают пароли в блокноты и записные книжки. Еще 13% (и 11% соответственно) хранят свои кодовые слова на компьютере, 12% (5%) записывают их в память телефона, 9% (10%) записывают и приклеивают на монитор, и лишь 7% (6%) респондентов используют для хранения паролей специальные приложения и сервисы.

Источник: [http://www.kaspersky.ru](http://www.kaspersky.ru/)

**Приложение 3**

       Сейчас у всемирной компьютерной сети пользователей больше, чем когда-либо ранее. Возможности ее использования также значительно расширились и включают электронные банковские услуги, онлайн-покупки и исследования, проводимые с помощью интернет-ресурсов. Кроме того, теперь мы рассматриваем виртуальное пространство как среду для общения. В последние годы в интернете появились социальные сети, такие как "Одноклассники.ru", "В контакте.ru" и др. Их участники обмениваются разнообразной информацией о своей личной жизни, а также музыкой, фотографиями и видеороликами.
К сожалению, чем больше пользователи сообщают о себе в сети, тем выше риск кражи их личных данных (identity theft) киберпреступниками, которые в дальнейшем мошенническим путем приобретают товары и услуги от имени пользователей и даже крадут деньги непосредственно с банковских счетов своих жертв.
       Поскольку пароли защищают конфиденциальную информацию, их важность трудно переоценить. Все ваши учетные записи в интернете должны быть защищены паролями. Но выбирать пароль нужно осмотрительно.
Пароль защищает ваши персональные данные от кражи, в том числе не позволяет злоумышленникам получить доступ к банковскому счету или другим электронным учетным записям и украсть ваши деньги.

        Надежный пароль снижает риск стать жертвой киберпреступников. Наши рекомендациипомогут вам создать пароли для ваших учетных записей в интернете.

Выбор надежного пароля

• Выбирайте пароли, которые вам будет легко запомнить и не придется записывать (в том числе вносить в файл на вашем компьютере). Такой файл может быть стерт, поврежден или украден киберпреступниками.

• Не используйте в качестве пароля реальные слова, которые киберпреступники могут найти в словаре. Используйте буквы как нижнего, так и верхнего регистра, а также цифры и другие символы – например, знаки препинания (хотя использование последних не всегда разрешено).
• Не прибегайте к "ротации" паролей, когда "пароль1", "пароль2", "пароль3" и т.д. используются попеременно для разных учетных записей.
• Если возможно, используйте в качестве пароля словосочетание, а не отдельное слово.
• Не используйте один и тот же пароль для разных учетных записей. В противном случае, подобрав только один пароль, злоумышленники получат доступ ко всем вашим онлайн-аккаунтам.

Пароль - это секрет

• Не используйте для защиты своих данных очевидные пароли, которые легко угадать: имя вашего супруга (супруги), ребенка, домашнего животного, регистрационный номер машины, почтовый индекс и т.п.

• Не сообщайте никому свой пароль. Если с вами связался (например, по телефону) представитель некой организации и попросил сообщить ваш пароль, не раскрывайте свои личные данные: вы не знаете, кто на самом деле находится на другом конце провода.

• Если онлайн-магазин или веб-сайт прислал вам по электронной почте сообщение с подтверждением регистрационной информации и новым паролем, как можно скорее зайдите на соответствующий сайт и смените пароль.

• Убедитесь в том, что установленное на вашем компьютере программное обеспечение для защиты от интернет-угроз блокирует попытки перехвата или кражи.

 Итак, выбирая пароль:

• Делайте его запоминающимся;
• Храните его в секрете;
• Не позволяйте с виду легальным организациям выманить его у вас обманным путем;
• Используйте одновременно буквы нижнего и верхнего регистра, цифры и другие символы;
• Не используйте один пароль для нескольких учетных записей;
• Не ротируйте пароли между разными учетными записями.

Источник: [http://www.kaspersky.ru](http://www.kaspersky.ru/)

**Приложение 4**

**Текст «Алгоритм создания надежного пароля»**

**Петров Иван Сергеевич 18 апреля 1982** года рождения для регистрации на сайте **superpochta.ru** может задать следующую последовательность:

1. Последние четыре символа адреса сайта прописными буквами (**superpochta.ru** = **A.RU**)
2. Сумма даты и месяца рождения (**18**+**4**=**22**)
3. Предпоследние три буквы отчества, набранные латинскими буквами (**Сергеевич** = **evi**)
4. Добавьте в конце восклицательный знак

В результате получается пароль **A.RU22evi!**

Тип урока - проект с элементами исследования. В начале урока учащиеся выходят на проблему: у них ненадежные пароли, которые не могут защитить личную информацию в интернете. В процессе урока ребята анализируют данные, делают выводы и представляют их в наглядном виде: какие пароли легко могут взломать и почему, как правильно хранить пароли, какие правила нужно знать, чтобы создать надежный пароль. После каждого этапа работы делятся своими выводами с одноклассниками. В конце урока учатся создавать надежный пароль по предложенному алгоритму.