Управление образования города Пензы
МКУ «Центр комплексного обслуживания и методологического обеспечения учреждений образования» г. Пензы
муниципальное бюджетное общеобразовательное учреждение
гимназия № 42 г. Пензы
(МБОУ ГИМНАЗИЯ № 42 Г. ПЕНЗЫ)

I Региональный конкурс научно-исследовательских работ
имени Д.И.Менделеева

Надежный электронный пароль - защита личных данных в сети Интернет

Выполнил:
Брякин Петр Сергеевич.
МБОУ гимназия № 42 г. Пензы,
4 а класс

Руководитель:
Алексеева Н.Н.,
учитель начальных классов,
МБОУ гимназия № 42 г. Пензы

Пенза 2021

Оглавление:

Введение

В нашем городе открылся Айти-куб, который я посещаю. Я хочу стать программистом и иду к своей цели. Меня заинтересовало направление киберследователь. Раньше о такой профессии я не слышал. Мы с папой решили поискать информацию в Интернете, оказалось, что более 10 крупных ВУЗов России обучают этой профессии.

Вот только оказалось, что учиться на киберследователя мне ещё рано, но изучить совместно с папой базовую безопасность в сети Интернет не только можно, а даже является необходимым в современном мире.

Я хочу изучить это направление и рассказать всем знакомым и друзьям о том, как важно держать свои личные данные в тайне от всемирной сети Интернет!

В этой работе мы рассмотрим такое важное направление безопасности, как пароли. Узнаем, что такое пароль, как давно появились пароли и многое другое об этом, казалось бы, простом слове.

Актуальность исследования.

Последние 10 лет очень быстрыми темпами развивается сеть Интернет, всё большее количество людей пользуются ею. В 2020 году, в связи с событиями мирового масштаба, онлайн индустрия развивается семимильными шагами, сейчас уже можно заказать через Интернет и оплатить пластиковой картой онлайн: продукты, готовую еду, миллионы товаров из разных категорий. Мои ровесники 8-9 лет начинают ежедневно использовать социальные сети, различные сервисы и игры. Но без знаний о безопасности, всё, выше сказанное, может привести к трагедии.

Цели работы: изучение информации о паролях**,** формулировка правил создания надежного пароля**.**

Гипотеза: я предположил, что не существует такой пароль, который бы абсолютно надежно защищал личные данные в сети Интернет.

Объект исследования: пароль, как защита личных данных в сети Интернет.

Предмет исследования: проверка надежности электронного пароля.

Для достижения поставленных целей мне нужно выполнить следующие **задачи**:

1. Найти в сети Интернет информацию о паролях.

2. Сформулировать правила создания надежного пароля.
3. Провести опрос среди одноклассников.
4. Рассказать одноклассникам о важности надежного пароля и правилах его создания.
5. Показать одноклассникам, как проверить надежность пароля при помощи сайта лаборатории Касперского.
6. Создать памятку о правилах создания пароля.

Методы исследования: теоретический анализ научной литературы и статей в сети Интернет; отбор информации; анализ; опрос; обобщение.

Теоретическая часть

Когда-то люди умели хранить секреты, но с приходом цифровой эры возможностей оставить что-либо конфиденциальным становится всё меньше. Данные о наших повседневных действиях: общении с друзьями, поездках в отпуск и покупках – всё это и многое другое записывается и хранится на серверах разных компаний и организаций. Всегда неприятно обнаружить, что личные сведения утекли в Интернет и все вокруг обсуждают ваши секреты. Сейчас в Интернете легче прославиться, чем может показаться. К сожалению, совсем не факт, что эта слава вам понравится. Мало кто вообще заботиться о конфиденциальности, а её отсутствие может обернуться для вас очень плохими последствиями. Часто пользователи сети Интернет становятся жертвами мошенничества, фальсификаций или кражи личных данных, незаконных операций, вымогательства, серьезного повреждения операционной системы устройства.

Защита личных данных – это важная проблема людей всех возрастов.

Так что же такое пароль?

Я обратился к Толковому словарю Ожегова. Пароль - это секретное условное слово (слова, фраза) для опознания своих караульным, а также в конспиративных организациях.

В Википедии я прочел, что слово «пароль» произошло от французского parole, что в переводе на русский означает «слово». Пароль – это условное слово или набор знаков, предназначенный для подтверждения личности или полномочий. Пароли часто используют для защиты информации от несанкционированного доступа. Несанкционированный доступ – это доступ к информации в нарушение должностных

полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

В большинстве вычислительных систем комбинация «имя пользователя – пароль» используется для удостоверения пользователя.

Из литературы я узнал, что пароли использовались с древнейших времен. Полибий (201 год до н.э.) описывает применение паролей в Древнем Риме следующим образом:

«То, каким образом они обеспечивают безопасное прохождение ночью выглядит следующим образом: и десяти манипул (основное тактическое подразделение легиона) каждого рода пехоты и кавалерии, что расположено в нижней части улицы, командир выбирает, кто освобождается от несения караульной службы, и он каждую ночь идёт к трибуну (командная должность в составе легиона), и получает от него пароль – деревянную табличку со словом. Он возвращается в свою часть, а потом проходит с паролем и табличкой к следующему командующему, который в свою очередь передает табличку следующему.»

Пароли использовались в компьютерах с первых их дней. Например, совместимая система распределения времени (CTSS) разработанная в вычислительном центре Массачусетского технологического института в 1961 году была одной из первых открытых систем и использовала команду LOGIN для запроса пароля пользователя.

Я узнал, что, как показывают исследования, около 40% всех пользователей выбирают пароли, которые легко угадать автоматически. Легко угадываемые пароли (123456), считаются слабыми и уязвимыми. Пароли, которые очень трудно или невозможно угадать, считаются более стойкими.

Есть некоторые критерии стойкости пароля:

1. Пароль не должен быть слишком коротким, поскольку это упрощает его взлом полным перебором. Наиболее распространенная минимальная длина – восемь символов. По той же причине он не должен состоять из одних цифр.
2. Пароль не должен быть словарным словом или простым их сочетанием, это упрощает его подбор по словарю.
3. Пароль не должен состоять только из общедоступной информации о пользователе.

В качестве популярных рекомендаций к составлению пароля можно назвать использование сочетания слов с цифрами и специальными символами (#, $, * и т.д.), использование малораспространенных или несуществующих слов, соблюдение минимальной длины.

В России существует федеральный орган исполнительной власти ФСТЭК (Федеральная служба по техническому и экспортному контролю), она выполняет специальные и контрольные функции в области государственной безопасности и подчиняется непосредственно президенту Российской Федерации. 11 февраля 2014 года ФСТЭК России был утвержден методический документ «Меры защиты информации в государственных информационных системах».

Из документа я узнал о паролях:

«… В случае использования в информационной системе механизмов аутентификации на основе пароля ... его характеристики должны быть следующими:

1. Длина пароля не менее шести символов,
2. алфавит пароля не менее 30 символов,
3. максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток,
4. блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 15 минут,
5. смена паролей не более чем через 180 дней.»

В этом документе ещё очень много информации, к сожалению, он устанавливает правила только для государственных информационных систем, а сайты в Интернет не обязаны придерживаться этих правил, поэтому необходимо самим пользователям дорожить своими данными и задумываться о безопасности.

Компания, предоставляющая менеджер паролей, NordPass опубликовала ежегодное исследование самых распространенных паролей этого года. Наиболее популярными среди них стали легко угадываемые комбинации цифр, например, «123456», а также слова «password», «qwerty», «iloveyou».

Составители списка оценили базу данных, включающую более 275 млн. паролей. Выяснилось, что только 44% из них являются уникальными.

В топ-10 самых популярных паролей вошли цифровые комбинации и простые слова:

1. 123456;
2. 123456789;
3. picture1;
4. password;
5. 12345678;
6. 111111;
7. 123123;
8. 12345;
9. 1234567890;
10. senha (означает «пароль» на португальском языке).

Если сравнить этот список с таким же прошлогодним рейтингом, можно сделать вывод, что люди по всему миру по-прежнему используют несложные и неуникальные пароли. Так, пароль «123456», который находится на первом месте в списке 2020 года, был вторым в 2019 году. Лидер прошлого года «12345» сейчас сместился на восьмое место.

У любого человека задумавшегося над надежностью пароля возникнет вопрос: как же хранить придуманный пароль, особенно, если он сложный?

Существуют различные способы хранения пароля, из самых надежных я хочу привести 2 способа, не являющиеся взаимоисключающими, то есть использовать можно их вместе:

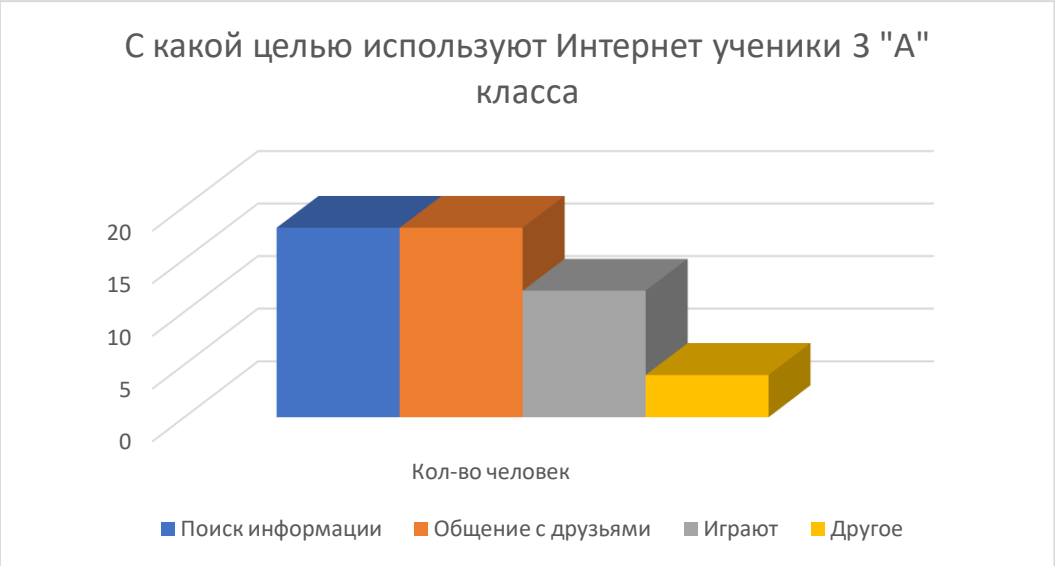
1. Записывать пароль на бумажном носителе, например, в блокноте, тетради, но ограничивать доступ к нему чужих людей. Например, у моего папы есть большая тетрадь для записей, на определенной странице которой он записывает все свои пароли. Тетрадь спрятана и найти её сложно.
2. Существуют специальные программы «менеджеры паролей». Например, у лаборатории Касперского есть **Kaspersky Password Manager** - менеджер паролей, который безопасно хранит данные под защитой одного мастер-пароля, с использованием облачной синхронизации всей хранимой информации. Все данные хранятся в специальном зашифрованном хранилище данных, доступ к которому можно получить только с помощью мастер-пароля. Мастер-паролем обязательно должен быть надежный, нигде больше не использующийся пароль,

для того чтобы его было просто запомнить можно воспользоваться способом создания надежного пароля из Приложения 2.

Практическая часть.

В своем классе я провел опрос о целях использования сети Интернет, выяснить, что знают ребята о надежности пароля в соц.сетях. Опрос показал, что все мои одноклассники пользуются Интернетом самостоятельно. (Приложение 1)

Используют же они его с разными целями:

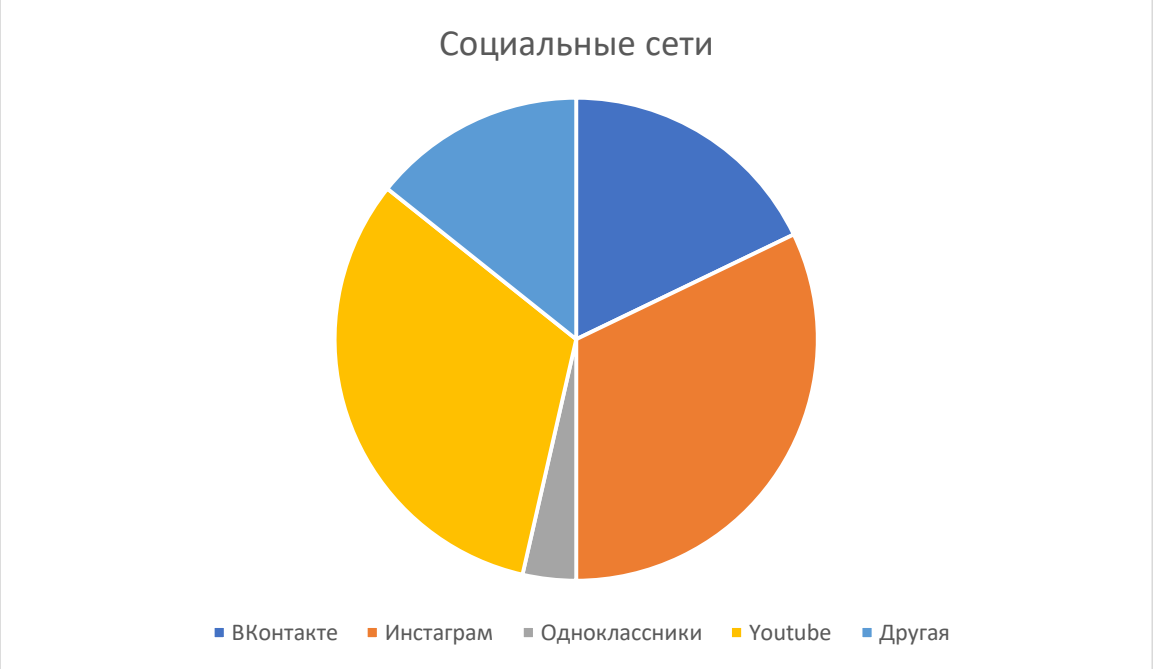


Этот график показывает, что мои одноклассники больше ищут информацию и общаются с друзьями, чем играют, я считаю, что это позитивная информация об учениках 3 «А» класса.

Зарегистрирован ли ты в социальной сети? Анализируя ответы на этот вопрос, я выяснил, из 28 опрошенных одноклассников, всего 6 не зарегистрированы ни в одной социальной сети, это 21 %.

Также я выяснил*, в каких социальных сетях ребята зарегистрированы*. В одной социальной сети зарегистрированы 14 человек, а оставшиеся 8 человек зарегистрированы в 2-х и более соц. сетях.

На графике ниже видно соотношение социальных сетей:

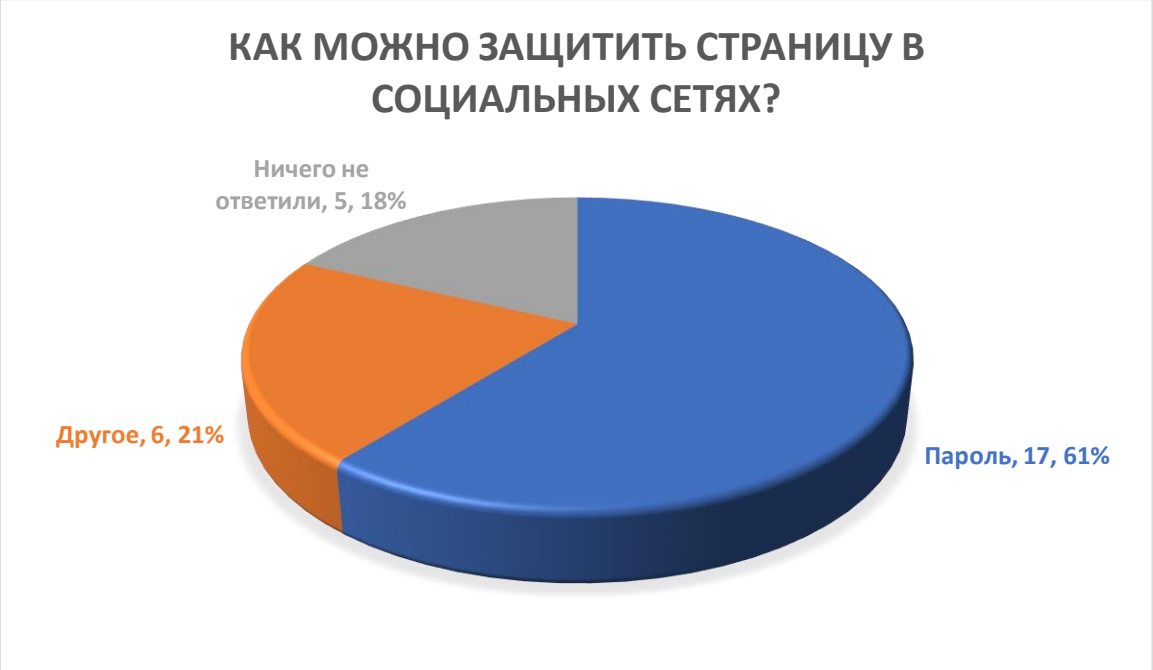


Большей популярностью в нашем классе пользуются такие социальные сети, как Инстаграм и Youtube.

Как ты считаешь, необходимо ли защитить свою страницу в социальных сетях?

На этот вопрос только 2 человека из 28 ответили - нет, даже те, кто не зарегистрирован в социальных сетях осознают необходимость защиты – это высокий показатель!

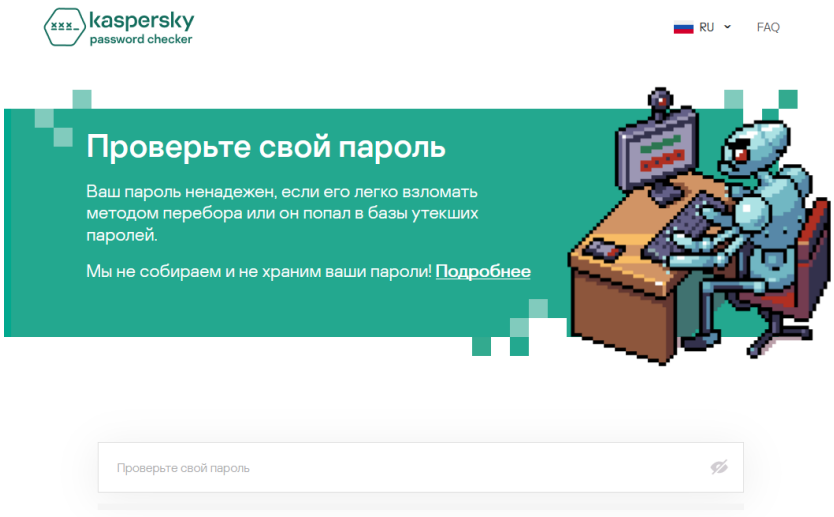
На вопрос: *как можно защитить страницу в социальных сетях*, подавляющее количество одноклассников ответили - поставить пароль, и редко было упоминание о его надёжности.



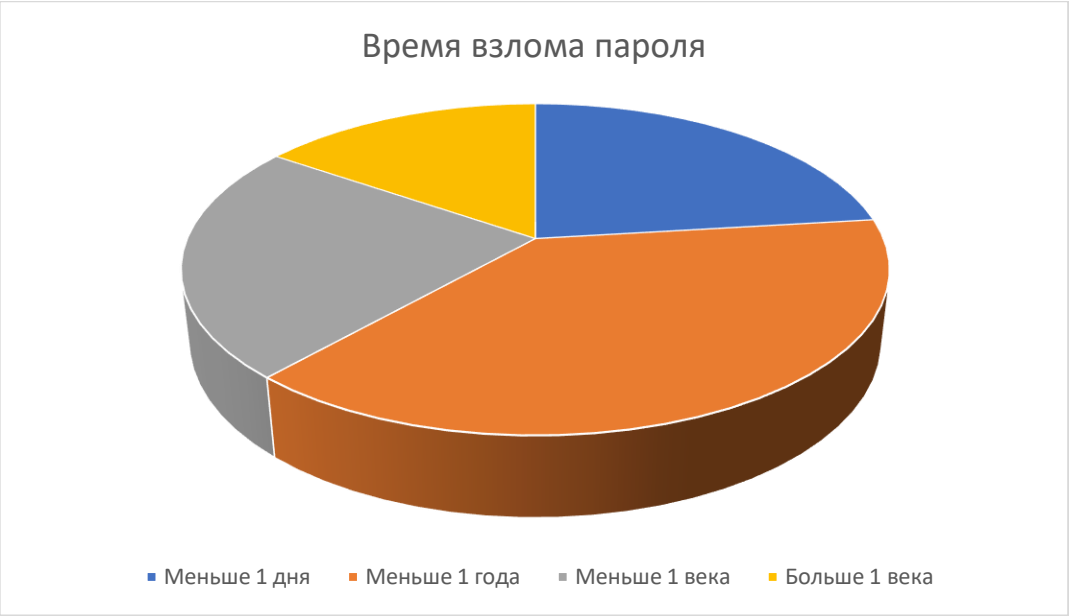
Из графика выше следует, что больше половины учеников знают о необходимости пароля, а некоторые даже упоминали его надежность. Большая часть тех, кто ничего не ответил, не зарегистрированы в социальных сетях и, скорее всего, пока не задумывались над этим вопросом.

24 ученика, примерно представляют, что такое пароль. 25 учеников класса считают, что их пароль надежный.

Я открыл сайт: https://password.kaspersky.com/ru/ «Проверьте свой пароль»



Последовательно ввёл пароли, предложенные одноклассниками, и получил такую статистику, показывающую соотношение предложенных паролей к времени их подбора техническими средствами:



Минимальное время взлома пароля составило 4 секунды, максимальное и это 3 пароля – более 10000 веков.

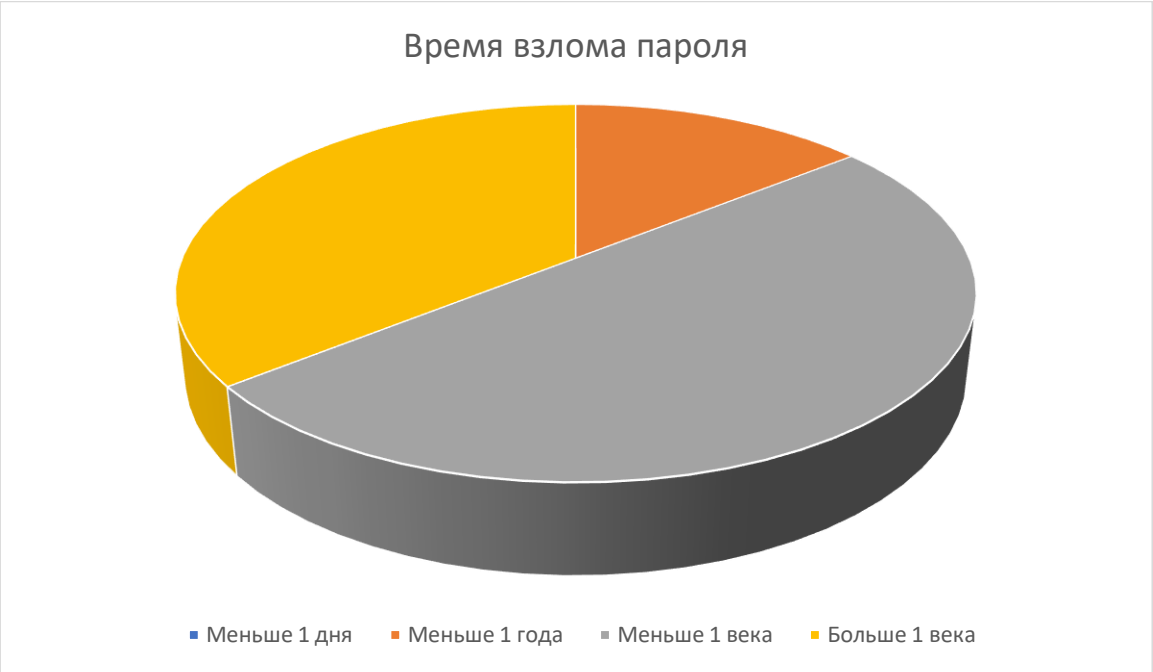
Из проведенной работы я делаю вывод, что много учеников 3 «А» класса используют надёжные пароли, но не все.

Мои одноклассники, как выяснилось из опроса, либо мало знают правила безопасности в Интернете, либо не знают совсем.

Практическое занятие.

Я решил познакомить своих одноклассников с работой сайта https://password.kaspersky.com/ru/ «Проверьте свой пароль» и провел мастер-класс по созданию надежного пароля для защиты аккаунта в социальных сетях. Я рассказал ребятам, что такое пароль, для чего его создают, как защитить свои личные данные страниц в социальных сетях. Каждый из ребят в конце занятия получил памятку.

По окончании работы ребята создали еще раз пароли, и мы вместе проверили их надежность на данном сайте. Мы убедились в том, что стали более грамотными в данном вопросе. Все ребята создали надежные пароли.



Я решил оформить памятку, которую распространил среди учащихся гимназии. (Приложение 2)

Планирую провести подобные мастер-классы для учащихся начальной школы гимназии.

Заключение.

Я провел актуальное исследование по теме. Сделал важные выводы, определил, что эта тема очень важная и нужная, особенно для моих сверстников. Как выяснилось, многие одноклассники не знают и не подозревают насколько важно защищать свои личные данные в сети Интернет. Иногда попадают в неприятные истории. Благодаря моим практическим действиям (выступление с презентацией, беседами, распространение памятки «Правила создания надёжного пароля»), я надеюсь, что моя работа улучшила ситуацию в этом вопросе и обратила внимание на его важность.

Моя гипотеза подтвердилась, теоретически не существует такого пароля, который нельзя было бы взломать, но надежным является любой пароль из более 8 цифр и английских букв и символов, и его сложно будет взломать автоматическими средствами.

Считаю, что мною достигнута цель работы: определить осведомленность учащихся о надежности пароля аккаунта в сети Интернет, я разработал рекомендации по созданию пароля.

Так же достигнуты все задачи, которые мы ставили перед собой:

1. Найти в сети Интернет информацию о паролях.
2. Сформулировать правила создания надежного пароля.
3. Провести опрос среди одноклассников.
4. Рассказать одноклассникам о важности надежного пароля и правилах его создания.
5. Показать одноклассникам, как проверить надежность пароля при помощи сайта лаборатории Касперского.
6. Создать памятку о правилах создания пароля.

Считаю, что материалы моей работы могут быть использованы на уроках окружающего мира и информатики в начальной школе. Планирую провести ознакомительные беседы и мастер-класс для учащихся всей начальной школы гимназии.

Список литературы

1. Мельников В. П. Информационная безопасность: Учеб. пособие для сред. проф. образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков; Под ред. С. А. Клейменова. — М.: Издательский центр «Академия», 2005. — 336 с.

2. Мельников В.П. Информационная безопасность и защита информации. [Электронный ресурс].

3. Гмурман, А.И. Информационная безопасность/ А.И. Гмурман - М.: «БИТ-М», 2006.- 387с.

4. Биячуев, Т.А. Безопасность компьютерных сетей / Т.А. Биячуев. - СПб: СПб ГУ ИТМО, 2009.- 161 с.

5. Сайт лаборатории Касперского: https://www.kaspersky.ru/

Приложение 1

Опросник

Надежный электронный пароль –

защита личных данных в сети Интернет.

1.Пользуешься ли ты самостоятельно Интернетом? (да, нет) Подчеркни нужное.

2. С какой целью ты используешь Интернет? Выбери ответ.

-поиск информации;

-общение с друзьями в сети;

-играю;

-другое.

3.Зарегистрирован ли ты в социальной сети? (Вконтакте, Инстаграм, Мой мир, Одноклассники, Ютуб и т.д.) (да, нет) Подчеркни нужное.

4.Как ты считаешь, необходимо ли защитить свою страницу в социальных сетях? (да, нет) Подчеркни нужное.

5.Как можно защитить страницу в социальных сетях?

_____

6.Что такое пароль?

_____

7.Предположим, что ты захочешь стать пользователем одной из сети и создать свою страницу, составь свой пароль:

_____

8.Ты считаешь надежным свой пароль? (да, нет) Подчеркни нужное.

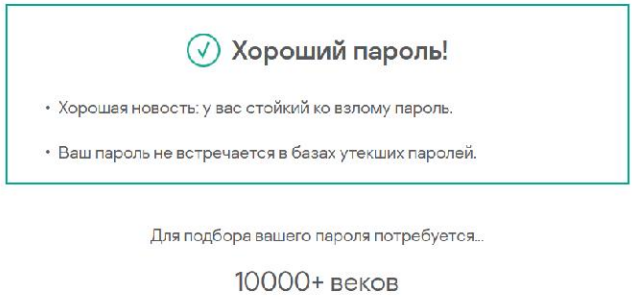
9.Знаешь ли ты правила безопасности в Интернете? Если да, то какие:

_____

_____

Дата: ____ октября 2020 года

Вы сделали всё по инструкции? Поздравляю у Вас надёжный пароль! Ваши личные данные в сети Интернет находятся в безопасности!



Не забывайте также о базовых правилах пользования паролем:

1. Никому не говорите свой пароль.
2. Следите, чтобы на Ваших устройствах не было вирусов.
3. Храните пароль в надежном месте.
4. Записывайте пароль только на бумаге, например, в блокноте.
5. Используйте такие подсказки на сайте (кодовое слово, ответ на секретный вопрос), которые не сможет угадать злоумышленник.
6. Всегда выходите из аккаунта после работы не на своём компьютере.

Для хранения созданного пароля используйте 2 способа:

1. Записывайте пароль в блокнот или тетрадь и не храните их на рабочем столе.
2. Воспользуйтесь специальной программой для хранения паролей – менеджером паролей. Одной из таких программ является Kaspersky Password Manager, скачать её можно здесь:

Для ПК:

Для Android:

г. Пенза 2021 год

МБОУ гимназия №42

ПАМЯТКА

«Правила создания и хранения надёжного пароля»

Автор: Брякин Пётр 3а класс

Не важно, какие правила к паролю предъявляет сайт на котором Вы регистрируетесь, всегда необходимо знать правила, которые я привожу в этой памятке.

Насколько бы не был надежным и защищенным пароль, всегда остаётся возможность взлома не Вашей учетной записи, а всего сайта, поэтому **первым правилом** надежности защиты личных данных будет:

Каждому сайту — по собственному уникальному паролю! То есть нельзя использовать один и тот же или мало отличающийся пароль в разных местах. Если Вы будете использовать один и тот же пароль, то всего одна утечка данных и все Ваши аккаунты будут под угрозой.

Вторым правилом будет длина пароля:

Длина пароля имеет большое значение. Пароль должен быть достаточно длинным, чем больше тем лучше, но в любом случае не менее 8 символов.

Третьим правилом является:

Пароль должен быть неоднородным! То есть должен состоять из разных символов — больших и маленьких букв, цифр, спецсимволов. Так он менее предсказуем, а значит — его труднее подобрать.

Четвертое правило:

Надежный пароль — это не обязательно комбинация случайных знаков, это последовательность символов, которую сложно взломать. И это не одно и то же! Лучше придумайте легко запоминаемый пароль, но из большого количества символов, например, более 12.

Один из способов создания надежного и легко запоминаемого пароля приведу ниже:

У каждого человека есть какой-нибудь любимый стишок или любимая фраза, например, каждый охотник желает знать, где сидит фазан, по ней проще всего запомнить цвета радуги, а можно её использовать и в создании пароля.

Берём первые буквы всех слов:

к о ж з г с ф

пишем их на английской раскладке клавиатуры, чередуем большие и маленькие и между ними вставляем спецсимвол, например, $:

Rj:pUcA

– эта комбинация взламывается за 33 века.

Эта комбинация будет базовой, для того, чтобы делать пароли для разных сайтов.

Например, возьмём социальную сеть ВК и какую-либо ассоциацию с этим сайтом, у меня ассоциацией будет цвет - синий, допишем его для сайта vk.com в конец пароля, не забываем о английской раскладке клавиатуры:

Rj:pUcAcbybq

– для взлома такого пароля нужно 10000+ веков.