КОМПЛЕКСНАЯ ПРОГРАММА ФОРМИРОВАНИЯ У ШКОЛЬНИКОВ ОСНОВ ЦИФРОВОЙ И ФИНАНСОВОЙ БЕЗОПАСНОСТИ

«Цифровой Я»

Материалы для проведения интерактивного урока

«Логины и пароли в цифровом мире»

Время проведения: 40 – 45 минут.
Оптимальное число участников: 25 – 35 человек.
Виды деятельности: рассказ, обсуждение (обмен мнениями), выполнение заданий.
Задачи:
1. Дать ученикам первоначальные представления о персональной информации и способах её защиты.
2. Познакомить с основными правила создания и использования паролей.
3. Учить пользоваться функциями двухфакторной аутентификации.
4. Учить детей работать с информацией, анализировать материал, принимать финансовые решения и оценивать свою работу.
5. Учить детей работать в группе, формулировать и обосновывать своё мнение и позицию.

Методические рекомендации
Методическая разработка рекомендуется для проведения урока «Логины и пароли в цифровом мире» в 5 – 11 классах. Класс может быть выбран на усмотрение организаторов. Перед проведением урока организаторам урока, ученикам старших (8 –11) классов, рекомендуется ознакомиться со структурой и содержанием разработки, а также проверить техническое оснащение кабинета.

Технические требования:
Компьютер, проектор, средство просмотра PowerPoint (или PDF).

Структура урока:

№	Этап (содержание)	Примерное время
1	Организационный	5 минут
2	Основной блок 1 (Персональные данные и их защита)	7 минут
3	Практический блок 1 (Создание сложного пароля)	7 минут
4	Основной блок 2 (Двухфакторная аутентификация, биометрическая защита)	10 минут
5	Практический блок 2 (Дискуссия о надёжности способов защиты информации)	10 минут
6	Завершающий (Рефлексия, домашняя работа)	6 минут

Сценарий урока «Логины и пароли в цифровом мире»

Организационный этап

ВЕДУЩИЙ
Здравствуйте, ребята!
Предлагаю вам стать участниками акции «Финансовая грамотность в цифровом мире».
Тема сегодняшнего урока – Логины и пароли в цифровом мире. (Слайд 1)
Как вы думаете какой пароль самый популярный? (Слайд 2)
Ответы учащихся. Обсуждение.
ВЕДУЩИЙ
К сожалению, многие люди не задумываются о безопасности своих данных и пользуются самыми простыми паролями, которые легко взломает любой мошенник. Целью нашего урока – узнать: зачем мы используем логины и пароли, что такое идентификация гражданина и зачем защищать свои персональные данные. Ваша задача – научиться создавать сложные пароли и использовать двухфакторную аутентификацию, а также выбирать безопасные способы хранения паролей. (Слайд 3)

Основной блок 1

Для начала предлагаю определить, зачем нам нужны логины и пароли? (Слайд 4)
Ответы учащихся. Обсуждение.
ВЕДУЩИЙ
Да, действительно, логины и пароли используются для проверки подлинности пользователя. Они позволяют сервисам и веб-сайтам удостовериться, что вы имеете право получить доступ к определенной информации или функциональности. Обычно, чтобы установить личность человека используют паспорт. В цифровом мире проверить паспорт у всех пользователей не представляется возможным, поэтому необходимо проходить проверку на каждом сайте отдельно. Сейчас многие сайты, платформы и сервисы объединят вход под одними учётными данными. Так, например, для доступа к разным ресурсам Яндекс, нужен всего один личный кабинет.
Большинство сайтов, платформ и приложений, которыми мы пользуемся требует от нас авторизации. Это значит, нам необходимо создавать личные кабинеты (аккаунты) с персональной информацией. Как вы думаете, какая персональная информация хранится в личных кабинетах? Приведите примеры.
Ответы учащихся. Обсуждение.
ВЕДУЩИЙ
Обратите внимание, как много примеров вы перечислили. И действительно, иногда в личных кабинетах хранится очень важная информация. Например, на сайте «Госуслуги». Знаете ли вы этот сайт? Через него каждый житель страны может получить важные государственные услуги. Например, оформить паспорт или записаться на приём к врачу. В личном кабинете на этом сайте хранится основная информация о человеке. Как думаете, что будет если этими данными завладеют мошенники? (Слайд 5)
Ответы учащихся. Обсуждение.
ВЕДУЩИЙ
Для предотвращения таких последствий необходимо устанавливать сложные пароли и пользоваться современными средствами защиты. Давайте начнём с паролей. (Слайд 6)
На слайде вы видите несколько паролей, подумайте, какие из них вы бы стали использовать?
Ответы учащихся. Просмотр ответов (Слайд 7) Обсуждение.
Примечание: на слайде с ответами есть вопрос про расшифровку. Ckj;ysqgfhjkm29 – это Сложныйпароль29 в другой раскладке клавиатуры.

Практический блок 1

ВЕДУЩИЙ
Предлагаю распределиться на группы и выполнить небольшое задание. Представьте, что завтра вашей группе необходимо провести мастер-класс для учеников начальной школы по составлению сложного пароля. Что каждой группе необходимо сделать? Разработать алгоритм придумывания сложного пароля. Записать (зарисовать) на листе. Закрепить на доске. Представить результат. (Слайд 8)
Выполнение задания. Сравнение и обсуждение результатов. (Слайд 9)
Рекомендации. Если вы располагаете достаточным количеством времени возможно предоставить слово группам. Если времени нет, задача ведущего просмотреть работы и кратко оценить их выполнение.
Дополнительно можно провести конкурс на самый сложный пароль. Его можно проводить в течение всего урока, предупредив об этом учащихся в начале. Если конкурс проводить не планируете, текст со слайда рекомендуется убрать.

Основной блок 2

ВЕДУЩИЙ
А теперь предлагаю рассмотреть способ, который помогает усилить защиту ваших данных. Он называется двухфакторная аутентификация. Возможно, вы уже сталкивались с таким способом. Он состоит из двух этапов. Сначала система спрашивает у пользователя пароля. А на втором этапе просит его подтвердить вход одним из способов. Это могут быть смс сообщения, пуш-уведомления или код в мобильном приложении. (Слайд 10) Как вы считаете, в чём преимущество такого способа защиты?
Ответы учащихся. Обсуждение.
Примечание: необходимо выделить 3-5 минут на выполнение задания (Составления списка сайтов и платформ, для которых требуется двухфакторная аутентификация). Обратите внимание учеников на то, что с этим списком им предстоит продолжить работу позднее.
ВЕДУЩИЙ
Всё, что мы рассмотрели до этого момента – можно назвать традиционной. Хочу обратить ваше внимание, еще на один способ защиты – биометрический.
Биометрическая система идентификации личности человека по отпечаткам его пальцев (дактилоскопия) получила распространение в XIX в. её родоначальником признаётся Уильям Джеймс Гершель, который, находясь в Индии, столкнулся с проблемой идентификации при выдаче жалования солдатам. они, пользуясь тем, что для европейца их лица малоразличимы, умудрялись получать жалование за один и тот же месяц по несколько раз. Метод дактилоскопии используется сегодня в современных смартфонах, где реализована функция разблокировки на основе отпечатка пальца его хозяина. А также смартфоны используют метод распознавания лиц.
Назовите, какими преимуществами обладает биометрическая защита? (Слайд 11)
Ответы учащихся. Обсуждение.

Практический блок 2

ВЕДУЩИЙ
Итак, мы с вами обсудили основные способы защиты данных: создание сложных паролей, двухфакторную аутентификацию и биометрическую защиту. Предлагаю провести обмен мнениями. Обсудите, какой способ защиты данных наиболее надежный?
Выскажите аргументированные мнения. (Слайд 12)
Ответы учащихся. Обсуждение.

Завершающий этап

ВЕДУЩИЙ
Благодарю за активное участие на уроке. Расскажите, что нового вы узнали на уроке? Что вам пригодится в дальнейшем? (Слайд 13)
Ответы учащихся. Обсуждение.
ВЕДУЩИЙ

Предлагаю вам в качестве домашнего задания провести чекап безопасности своих персональных данных. Проверьте двухфакторную аутентификацию в своих аккаунтах и проанализируйте пароли. (Слайд 14)
Урок закончен. Спасибо за внимание.