Автор (ФИО, образовательное учреждение):	Соседкина Наталия Валерьевна МБОУ гимназия 3 в Академгородке города Новосибирска
Название модуля и тема внутри модуля (ненужное удалить):	Модуль 1. Технические аспекты использования Интернета. ● Надежные пароли
Форма (ненужное удалить):	фрагмент урока
Класс:	8-9
Тема урока:	Проверка надёжности пароля
Цель:	Показать основные подходы к измерению надёжности пароля. Оценить надёжность паролей, аналогичные своим. Задуматься над важностью проблемы грамотного выбора пароля.

Упражнение 1. Придумаем плохой пароль

Задача:	Разобраться с популярными ненадёжными паролями,
Необходимые медиа материалы:	проекторное оборудование, маркеры для доски
Время проведения:	10-12 минут

Процедура проведения

Пароль – тайна пользователя. Но у организаторов популярных сайтов с регистрацией всегда была возможность проанализировать качество паролей. Их исследование выявило ТОП-1000 популярных паролей. После серии массовых утечек паролей у желающих. Появилась возможность проанализировать несколько миллионов паролей. Но ТОП-1000 не дрогнул. Каждый девятый пользователь выбрал пароли из этого списка.

Ученики разбиваются на группы по 3 человека. Каждая группа придумывает 10 популярных ненадёжных паролей длины не менее 6 символов. Записывает эти пароли на доске, затем аргументирует свой выбор.

Проходит обсуждение, какие же пароли самые популярные, как часто пароль связан с информацией о его владельце?

Далее ученикам показывают картинку с TOP-1000.

Обсуждение

Какие пароли самые популярные?

Если знать человека, чей пароль подбирается, насколько вырастают шансы взломать пароль?

Приложение

Картинка с сайта <https://xato.net/wp-content/xup/passwordscloud.png>

Подводя итоги

Нельзя ставить на важные аккаунты простые пароли. Какие именно нельзя – мы поняли. Пришло время понять – какие можно.

Упражнение 2. Оценим надёжность пароля

Задача:	Разобраться с оценкой надёжности пароля, оценить надёжность пароля, аналогичного своему
Необходимые медиа материалы:	Компьютер с доступом в интернет, проекционное оборудование, маркеры для доски
Время проведения:	12-15 минут

Процедура проведения

Проблемный полилог:

Программа подбора паролей сначала проверяет пароль на стандартных топовых вариантах. Мы уже поняли, что популярны клавиатурные последовательности. Хороши также слова из словарей. Далее те же самые слова, но с заменами «to» на «2» и аналогичными. Далее – вариации с именем пользователя. Для российских пользователей надо также проверить словарь на написание его в транслитерации. Сколько времени займёт это у компьютера? Современные технические возможности позволят сделать это за секунды. А что может заметно удлинить поиск? Полный перебор вариантов.

Для этого в информатике используется такой термин как энтропия – «анти-хаос».

Цитата из Википедии (если урок проводится для учеников старших классов):

В компьютерной индустрии обычно оценивают сложность пароля в терминах [информационной энтропии](#) (понятие из [теории информации](#)), измеряемой в битах. Вместо количества попыток, необходимых, чтобы точно угадать пароль, берется логарифм по основанию 2 от этого числа и называется количеством «битов энтропии» в пароле. Пароль со, скажем, 42-битной сложностью, посчитанной таким путем, будет соответствовать случайно сгенерированному паролю длиной в 42 бита. Другими словами, чтобы взломать пароль с 42-битной сложностью, необходимо произвести 2^{42} попыток, исчерпав все возможные варианты методом полного перебора. Таким образом, добавление одного бита энтропии к паролю удваивает количество необходимых догадок, что делает задачу атакующего в два раза сложнее. В среднем, атакующий должен будет проверить половину из всех возможных вариантов пароля, до того как найдет правильный. ([Закон больших чисел](#))

Добавление 1 буквы к длине пароля увеличит надёжность в 500 раз. Если буквы в пароле случайные, то энтропия сильно возрастает. Но случайные пароли сложно запомнить. Противоречие.

Работа за компьютером. Демонстрация программы оценит ваш пароль по многим параметрам. Привлекая знания английского языка, догадайтесь, что означают выданные программой характеристики.

<https://dl.dropboxusercontent.com/u/209/zxcvbn/test/index.html>

Потестируйте разные пароли, только не стоит вбивать туда свои настоящие.

Другой скрипт для тестирования паролей позволяет видеть, сколько бит даёт каждый символ пароля и почему. Попробуйте добавлять к паролю разные символы и оценивать как возрастает уровень надёжности.

<http://earninguide.biz/passwordmeter.php>

Обсуждение

Что значительно увеличивает уровень надёжности пароля?

Как найти компромисс между сложностью пароля и его запоминаемостью?

Приложение

Перевод характеристик в статье «zxcvbn: реалистичная оценка надёжности пароля»

<http://habrahabr.ru/company/abbyy/blog/149396/>

On-line – тестировщики паролей на сайтах

<https://dl.dropboxusercontent.com/u/209/zxcvbn/test/index.html> и

<http://earningguide.biz/passwordmeter.php>

Подводя итоги

Резюме учителя (вывод) по теме.

Научитесь составлять надёжные пароли. И разумно оценивать их устойчивость к взлому.