Муниципальное общеобразовательное учреждение «Стрелецкая средняя общеобразовательная школа Белгородского района Белгородской области имени Героя Советского Союза А.Е.Черникова»

**Методическая разработка классного часа**

**«Безопасность в сети интернет»**

**Автор-составитель: Коновалова Татьяна Алексеевна,**

Учитель технологии, биологии и химии, классный руководитель

с. Стрелецкое

2021 год

**Аннотация:** в современном мире злоумышленникам не требуется много времени, чтобы узнать многое о будущей жертве, ведь многие люди выкладывают о себе в интернете слишком много информации. Важно знать, как обезопасить себя и свои личные страницы.

**Категория обучающихся:** методическая разработка предназначена для работы с обучающимися 12-16 лет (5-9 классы общеобразовательной школы).

**Цель:** содействие формированию у учащихся элементарных представлений о безопасности в интернете, проверка личных страниц в социальных сетях.

**Задачи:**

*1. Обучающие:*

- познакомить учеников с угрозами и рисками в интернете;

- сформировать умение определять социальные характеристики и индивидуальные особенности людей

- познакомить с признаками опасного поведения на основании аккаунтов в социальных сетях;

- сформировать способность к успешной самопрезентации и формированию позитивного имиджа в социальных сетях.

*2. Развивающие:*

- познакомить учеников с основами исследовательской деятельности;

- начать развивать психофизиологические качества обучающихся, такие как память, внимание, логическое мышление;

- способствовать организации культурного досуга путем активного использования ресурсов.

*3. Воспитательные:*

* формировать волевые качества для успешной деятельности, такие как усидчивость, настойчивость, терпение, самоконтроль;
* формировать коммуникативную культуру учащихся, умение продуктивно работать в команде.

**Ожидаемые результаты:**

*1. Обучающие:*

- умение определять рискованное и опасное поведение и угрозы в интернете и понимание как их можно идентифицировать в социальных сетях;

- понимание правил безопасного поведения в интернете, правильного и безопасного использования персональных данных, защиты от вредоносных воздействий.

*2. Развивающие:*

- знание основ исследовательской деятельности;

- хорошая динамика в развитии психофизиологических качеств.

*3. Воспитательные:*

- выполнение работы самостоятельно, планируя свои действия и координируя их с действиями группы.

**Материалы и оборудование**: презентация к занятию, проектор, компьютеры на каждого ученика или группу до 3 человек.

**Ход занятия**

 **Приветствие педагога, объяснение темы классного часа с помощью дискуссии.**

*Введение в проблему с помощью вопросов для учащихся:*

 Расскажите пожалуйста, какими ресурсам в интернете вы чаще всего пользуйтесь, на какие сайты заходите чаще?

 Уверены ли вы, что личные данные, которые вы разместили в интернете под надежной защитой?

 Почему вы уверены или не уверены в защищённости данных?

 Что может стать причиной утечки данных? *(вывести на проблему кибератак, программного обеспечения и невнимательности)*

**Основная часть**

Согласно исследованиям, почти 62% жителей нашей страны пользуются социальными сетями с той или иной периодичностью:

* 41% опрошенных заходят ежедневно,
* 14% — несколько раз в неделю,
* 4% — несколько раз в месяц.

 Молодежь (18-24 года) является самым активным пользовательским кластером, среди них доля ежедневного пользования составляет 82% (для сравнения среди людей 60+ лет эта цифра составляет 15%).

У кого из вас есть страничка в социальной сети? При регистрации вы читали пользовательское соглашение? Чаще всего люди его просто пролистывают, но что важного можно узнать из этого документа?

*Дискуссия на тему пользовательского соглашения.*

Действительно, пользовательское соглашение необходимо для того, чтобы понять свои права и обязанности и самой социальной сети.

К сожалению, многие аккаунты подвергаются взломам и причин этого великое множество. Причем атакам подвергаются не только страницы обычных людей, но и политиков, других известных личностей. Зачем это делается?

*Обсуждение*

Давайте проверим, подвергалась ли взлому ваша страница в социальной сети с помощью специального сервиса. (<https://haveibeenpwned.com/>).

Отлично, завершаем проверку. И давайте подумаем, что может обезопасить вашу страницу от взлома? *Выход на тему безопасного пароля.*

Безопасный пароль является основой безопасности личных данных в интернет пространстве. Для его создания лучше применять следующие правила:

* комбинировать в пароле более шести прописных и строчных букв, цифры и знаки препинания;
* длинный пароль взломать сложнее;
* не следует использовать один пароль ко всем страницам;
* не использовать при составлении пароля личную информацию (дату рождения, номер телефона и прочее);
* не сохраняйте информацию о паролях в компьютерах, доступ к которому имеется не только у вас;
* периодически обновляйте пароли.

 С какими из перечисленных правил вы согласны? С какими трудно согласиться?

 Мы разобрались в принципах формирования безопасного пароля. Но остался вопрос: как его запомнить?

 Теперь давайте обсудим риски, который могут возникнуть при размещении в интернете личной персональной информации, такой как адрес, информации о месте обучения, электронная почта и прочее?

*Обсуждение*

 Давайте вместе составим таблицу, откуда может быть похищена информация о нас, какого она может быть содержания, и кто может ее выложить.

|  |  |  |
| --- | --- | --- |
| Интернет-ресурс | Содержание | Кто выкладывает? |
| *Социальная сеть* | *телефон* | *Я сам* |
|  |  |  |

 Ученые провели исследование школьников, согласно которому получить полную информацию о человеке можно не только по прямо предоставленным данным, но и косвенным сведениям. Учащиеся выставляли в сеть информацию о своих оценках, школе, классе, студенты о ВУЗе, курсе и программе обучения. По имени, фамилии и конкретному учебному заведению можно было идентифицировать человека на 18%. Но если добавит информацию о друзьях, то показатель увеличивался до 88-93%.

 По каким еще признакам и критериям можно идентифицировать человека в сети? Что можно посоветовать по использованию настроек приватности в социальных сетях?

*Обсуждение*

 Общение в сети подразумевает новые знакомства, общение с людьми, которых в реальной жизни вы можете и не встретить. Именно в такой ситуации есть риск разглашения какой-либо важной информации о себе или свое семье. Расскажешь интернет-другу о планируемой поездке на море, а в ваше отсутствие ограбят квартиру. Совпадение?

 Кроме этого есть риск подвергнуться запугиванию, оскорблениям и прочим неприятностям. Шантаж, эксплуатация, - далеко не самые страшные вещи, которые происходят с детьми при общении с виртуальными «друзьями». Чаще всего это даже не сверстник, как он представляется. Поэтому при знакомствах в сети следует быть бдительным и аккуратным.

В завершение нашего занятия давайте пройдем тест, составленный Роскомнадзора <http://персональныеданные.дети>

**Подведение итогов занятия**

1. Вопросы детям:
* что нового узнали, что понравилось?
* какие вы можете дать рекомендации пользователям интернета в вопросе безопасности?
1. Оценка педагогом работы детей на занятии.

# **Список информационных источников**

1. Солдатова Г., Рассказова М., Лебешева М., Зотова Е., Рогендорф П. Дети России онлайн. Результаты международного проекта EU Kids Online II в России. М.: Фонд Развития Интернет, 2013.
2. Солдатова Г.У., Шляпников В.Н., Журина М.А. Эволюция онлайн рисков: итоги пятилетней работы линии помощи «Дети онлайн» // Консультативная психология и психотерапия. 2015. № 3. С. 50-66.
3. Абаев А.В. Безопасности при работе сети интернет [Электронный ресурс] // Научное сообщество студентов XXI столетия. ТЕХНИЧЕСКИЕ НАУКИ: сб. ст. по мат. XXXVIII междунар. студ. науч.-практ. конф. № 1 (37). URL: <https://sibac.info/studconf/tech/xxxviii/46531> (Дата обращения 14.09.2019).
4. Безопасность в Интернете. Электронный курс [Электронный ресурс]. URL: <http://www.intuit.ru/studies/courses/3462/704/info> (Дата обращения 03.10.2019)