Управление образования Администрации Сосновского муниципального района

Муниципальное образовательное учреждение

Сосновская средняя общеобразовательная школа №1

ПРОЕКТ

**ОБЕСПЕЧЕНИЕ ЛИЧНОЙ БЕЗОПАСНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ**

Автор: Силаева Ксения Александровна

ученица 6а класса

руководитель: Е. С. Ильина,

учитель информатики высшей категории

п. Сосновское

2015

**Оглавление**

Введение………………………………………………………………………….. 3

Основные понятия социальных сетей……………………...………………….. 4

История………………………………………………………………………… 4

Плюсы и Минусы социальных сетей……………………………....………… 4

Опасности социальных сетей………………………………………………… 5

Правила……………………………………………………….……………..… 6

Заключение……………………………………………………………………….. 8

Список источников информации……………………………………………..... 9

Приложение 1. Флаер «Правила безопасности в социальных сетях»…….….10

Приложение 2.Скриншот моей страницы «Вконтакте»……………………..11

**Введение**

Наша жизнь постепенно уходит в Интернет. В нем можно найти многое: развлечение, разнообразные форумы и чаты, социальные сети и многое другое. Но Интернет - мир, который не только интересен и увлекателен, но и полон опасностей. Тема безопасности пользователя сети Интернет очень актуальна, особенно для подростков, так как мы очень много времени проводим в Интернете, а значит, подвергаем себя опасности. Социальные сети – наиболее распространенное «место встречи» людей. В социальных сетях можно найти своих одноклассников и приобрести новых друзей. В некоторых социальных сетях есть развлечения, такие как игры, сообщества или группы, музыка и видео. В социальных сетях вы можете общаться с друзьями и приятелями. В разных сообществах или группах вы можете узнать что-то новое и интересное. Также вы сможете создать свою группу. Но в социальных сетях есть и опасности, такие как хейтеры и троллинг. Личную страничку могут взломать. Думаю, чтобы не подвергаться таким опасностям, нужно больше знать о структуре социальных сетей, опасностях и способах защиты.

**Цель проекта:** создать памятку с правилами безопасности в социальных сетях.

**Задачи:**

1. Узнать, почему людям нравятся социальные сети.

2. Какие существуют плюсы и минусы социальных сетей.

3. Узнать, собрать и систематизировать правила безопасности в социальных сетях.

**Основные понятия социальных сетей**

**Что такое социальные сети?**

Социальная сеть - это платформа, онлайн сервис или веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений. Безопасность в социальных сетях и вообще на просторах сети Интернет все больше и больше волнует пользователей. Надо обязательно помнить о защите своего компьютера и своих личных данных. Если не задумываться, то социальная сеть – просто удобный способ общения с друзьями, легко отправлять сообщения, смотреть и комментировать фотографии. В первую очередь, это сайты, разработанные с целью познакомить и собрать людей с общими интересами, дать им возможность общаться на различные темы, выкладывать и обсуждать фото и видео, добавлять друг друга в друзья или недруги, загружать и слушать музыку и т.д. Одним из плюсов социальных сетей является возможность найти давно потерянных друзей, родственников.

**История**

Популярность в Интернете социальные сети начали завоёвывать в 1995 году, с появлением американского портала Classmates.com. Проект оказался весьма успешным, что в следующие несколько лет спровоцировало появление не одного десятка аналогичных сервисов. Но официальным началом бума социальных сетей принято считать 2003-2004 года, когда были запущены LinkedIn, MySpace и Facebook.

**Плюсы и Минусы социальных сетей**

Плюсы

1.В социальных сетях можно писать sms-сообщения бесплатны.

2. Есть игры.

3. Есть интересные группы.

4. Можно слушать песни и смотреть видео бесплатно.

5. На мобильных версиях можно ставить графический ключ (как средство защиты при краже телефона).

6. Можно выкладывать свои фотографии, их будут комментировать и «лайкать» (выражать симпатии).

Минусы

1. Вас могут «взломать».
2. У вас могут украсть ваши личные данные для плохих целей.

**Опасности социальных сетей**

Многие люди не понимают, что информация, размещённая ими в социальных сетях, может быть найдена и использована кем угодно, не обязательно с благими намерениями. Информацию об участниках социальных сетей могут найти их работодатели, родственники, сборщики долгов, преступники и так далее. Судебные приставы иногда используют социальные сети, чтобы найти неплательщиков или получить сведения об их имуществе.

Известен случай проявления психосоматических расстройств на почве зависимости от общения в социальных сетях — в Белграде пользователь Снежана Павлович (Snezhana Pavlović) попала в психиатрическую клинику после того, как её заметка в социальной сети Facebook не вызвала интереса среди её друзей. Врачи клиники назвали этот случай «синдром Снежаны», объясняя поведение пациентки как обычный стресс от неудовлетворенности своей социальной потребности в современном мире.

Некоторые работодатели запрещают пользоваться социальными сетями - не только ради экономии, но и чтобы воспрепятствовать утечке информации. Не переходите по незнакомым вам ссылкам, потому что можно скачать на свой компьютер вирус. Старайтесь контролировать информацию о себе, потому что есть люди, которые могут вашу информацию выдать за свою. Старайтесь отправлять сообщение близким или хорошо знакомым вам людям, потому что иначе ваше сообщение могут использовать в своих корыстных целях или просто, чтобы навредить вам. Не стоит «добавлять в друзья» всех подряд, потому что можно наткнуться на плохих людей. Не стоит регистрироваться во всех социальных сетях подряд, потому что сайт может быть поддельным и позволит украсть ваши личные данные. Когда вы публикуете вашу личную информацию, нужно понимать, что ваша информация может быть сохранена кем-нибудь чужим и необязательно дружелюбным по отношению к вам. Старайтесь не скачивать никаких дополнений к социальным сетям, потому что можно «поймать» вирус, который сильно повредит ваш компьютер. Не стоит посещать социальные сети с рабочего места, потому что может произойти утечка деловой информации, за которую несет ответственность организация и лично работник. Скачайте антивирус для социальных сетей, чтоб вас не могли взломать или украсть ваши личные данные. Не пишите номера телефонов незнакомым вам людям. Не регистрируйтесь и не пишите свой номер на неизвестных вам сайтах, если же вы напишете, то с вашего номера могу снять немалые деньги, которые вы могли бы потратить на другие полезные услуги.

Часто для преступных целей используются страницы знаменитых людей, ведь все хотят «добавить в друзья» знаменитого артиста или спортсмена. Нужно понимать, что настоящие знаменитости с кем попало не дружат, а вы для них - неизвестно кто! Администраторы социальных сетей сами стараются защитить своих пользователей от поддельных страничек –«фейков», отмечая оригинальную страницу знаменитости специальным знаком (рисунок 1).



Рисунок 1. Знак «подтвержденной» страницы знаменитости

**Правила**

Изучив несколько источников информации, я учла рассмотренные выше опасности, подстерегающие нас в социальных сетях и выделила правила, которые считаю самыми важными и актуальными, в первую очередь для себя:

1. Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях от других пользователей или друзей.

2. Контролируйте информацию о себе, которую вы размещаете.

3. Не думайте, что сообщение, которое вы получили, было отправлено тем, кого вы знаете, только потому, что так написано.

4. Чтобы не раскрыть адреса электронной почты своих друзей, не разрешайте социальным сетям сканировать адресную книгу вашего ящика электронной почты.

5. Вводите адрес социальной сети непосредственно в адресной строке браузера или используйте закладки.

6. Не добавляйте в друзья в социальных сетях всех подряд.

7. Не регистрируйтесь во всех социальных сетях без разбора.

8. Учитывайте тот факт, что все данные, опубликованные вами в социальной сети, могут быть кем-то сохранены.

9. Проявляйте осторожность при установке приложений или дополнений для социальных сетей.

10. Старайтесь не посещать социальные сети с рабочего места.

11. Расскажите вашим друзьям, знакомыми родственникам об опасностях, которые могут подстерегать их в социальных сетях.

12. Не посещайте не «подтвержденные» страницы. Если вы случайно оказались на такой странице, покиньте ее как можно быстрее.

13. Никогда не рассказывай о себе незнакомым людям в Интернете.

14. Никогда не отвечай на сообщения от незнакомцев в Интернете.

15. Всегда спрашивай родителей или родственников о незнакомых тебе вещах.

**Заключение**

Я считаю, что достигла поставленной цели. Насколько я знаю, мне и моим одноклассникам нравятся социальные сети, поэтому меня заинтересовала именно эта тема. Очень важна информация о плюсах и минусах социальных сетей, как обезопасить себя от взломов и других опасностей. Надеюсь, что собранная мной информация будет полезна идля моих друзей. После проделанной работы мне я стала увереннее в социальных сетях, потому что больше узнала о них. Думаю, есть еще много интересной и полезной информации, поэтому я продолжу свое исследование такого сложного объекта как социальные сети. Продуктом моей деятельности стал небольшой флаер – памятка с правилами безопасности для распространения среди друзей. Его я сделала в графическом редакторе Paint. Чтобы разместить больше правил, можно сделать буклет. Это станет следующим этапом моего проекта. Также перечень правил безопасности я разместила на своей странице в социальной сети «Вконтакте», чтобы мои друзья могли их видет, оставить на своей стене как памятку и постоянно пользоваться ими.

**Список источников информации**

## 1. Правила безопасности при использовании социальных сетей

http://www.microsoft.com/ru-ru/Security/online-privacy/social-networking.aspx

2. Безопасность в социальных сетях. http://alphaland.in/bezopasnost-v-sotsial-ny-h-setyah/

3. Безопасность в социальных сетях. http://ihaker.ru/security-in-social-networks/

4. Социальная сеть. https://ru.wikipedia.org/wiki/%В1%УУ%А6%У8%У0% УИ%АС%УВ%У0%АА\_%А1%У5%А2%АС

5. Что такое социальная сеть. http://ledsoft.info/articles-ru/internet-ru/dialogue-ru/93-socialnetworks/87-socialnetworks.

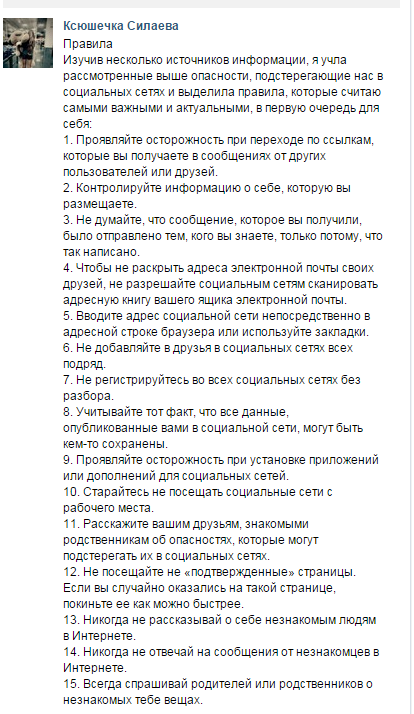
**Приложение 1**

**Флаер «Правила безопасности в социальных сетях»**



**Приложение 2**

**Скриншот моей страницы «Вконтакте»**

****