**КОНСУЛЬТАЦИЯ ДЛЯ РОДИТЕЛЕЙ**

**«ПОДРОСТКИ В СОЦИАЛЬНЫХ СЕТЯХ: БЕЗОПАСНОЕ ПОВЕДЕНИЕ»**

Подготовил классный руководитель

6 класса Бурдук А.Г.

Дата проведения – 17.01.2023

Целевая группа – родители учащихся 6 класса

**Цель:** сформировать у родителей навыки контроля за использованием несовершеннолетними сети Интернет.

**Задачи:**

обеспечение информационно безопасности несовершеннолетних и их родителей путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

предупредить криминальные посягательства на учащихся.

развивать информационно-коммуникативные компетенции у родителей несовершеннолетних.

**Методы:** беседа, работа в группе.

**Оборудование:** ноутбук, проектор, экран, презентация в программе POWER Point, раздаточный материал.

Проблема безопасности подростков в сети интернет важна и актуальна, потому что стремительное развитие компьютерных технологий, наряду с глобальной информатизацией общества, качественно меняет окружающую нас жизнь и порождает множество новых проблем, в частности, проблему формирования информационной культуры и безопасности среди подрастающего поколения.

На данный момент в мире возникло устойчивое понимание того, что проблема безопасности детей в интернете — это проблема, требующая срочного вмешательства специалистов. Новым и самым эффективным механизмом решения этой проблемы может и должно стать формирование информационной культуры личности — родителей и детей, а также профессиональной информационной культуры учителей.

Взрослым важно помнить, что даже самые искушенные дети не видят опасностей Интернета и не осознают рисков его использования. Существуют различные мнения о том, когда нужно давать детям доступ в Интернет. Зарубежные специалисты сходятся в том, что запрет на Интернет может быть действенным только до тех пор, пока это не ограничивает потребности ребенка в сфере образования.

По оценке европейских исследователей самую большую угрозу представляет выманивание и распространение личной информации в Сети. Больше половины опрошенных старшеклассников часто дают в интернете номер своего домашнего телефона (79%), номер мобильного (65%), номер школы или класса (60%), свои фотографии и фотографии родственников (58%), адрес своей электронной почты (51%).

Таким образом, ученые констатируют недостаточный уровень информированности детей о безопасности в Интернете при высоком уровне рисков, которым подвергает себя ребенок. К тому же совершенно недостаточным является уровень вовлеченности учителей в процесс воспитания культуры безопасного пользования Интернетом среди детей, в том числе из-за проблемы осведомленности.

Для того, чтобы обеспечить безопасность использования подростками социальных сетей важно выявить основные проблемы связанные с их использованием.

**Общая характеристика социальных сетей, как средства взаимодействия подростков**

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты.

«Новый тренд» в Интернете, социальные сети, начались в 1995 году с американского портала Classmates.com («Одноклассники» являются его русским аналогом). Проект оказался весьма успешным, что в следующие несколько лет спровоцировало появление десятка похожих сервисов. Но официальным началом бума социальных сетей принято считать 2003—2004 годы, когда были запущены LinkedIn, MySpace и Facebook. В Россию мода на социальные сети пришла двумя годами позже — в 2006-м, с появлением Одноклассников и ВКонтакте.

И если LinkedIn создавалась с целью установления деловых контактов, то владельцы MySpace и Facebook сделали ставку в первую очередь на удовлетворение человеческой потребности в самовыражении. Социальные сети стали своего рода Интернет-пристанищем, где каждый может найти базу для создания своего виртуального «Я». При этом каждый пользователь получил возможность не просто общаться и творить, но и делиться плодами своего творчества с многомиллионной аудиторией той или иной социальной сети.

Однако многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями. Информацию об участниках социальных сетей могут найти их работодатели, бывшие или настоящие жены или мужья, сборщики долгов, преступники, правоохранительные органы и так далее.

Известен случай проявления психологического расстройства на почве зависимости от общения в социальных сетях. В Белграде девушка Снежана Павлович 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 социальной потребности индивидуума в современном мире.

**Социальные сети как угроза безопасности жизнедеятельности подростка**

Самый главный риск общения в социальных сетях – это потеря персональных данных и информации для доступа к аккаунту. Потеря контроля за профайлом (краткие сведения о пользователе: дата рождения, имя, ник, когда зарегистрирован, увлечения и прочая информация) может привести к различным последствиям, таким как рассылка спама и зараженных файлов от твоего имени или опубликование твоей переписки с друзьями;

* Информация, которая появляется в интернете в отношении подростка, может очень повлиять на него сейчас и в будущем. Например, подросток может показывать, что ты лентяй или может быть очень вульгарным в общении в социальной сети, что характеризует тебя с плохой стороны. Именно такой вывод сделает менеджер по персоналу, который будет принимать решение о приеме на работу.
* Подросток может заинтересовать не только кибер, но и других преступников. Например, размещая информацию о своей квартире, благосостоянии своей семьи, сообщая куда он с семьей поедет на каникулы, ребенок может заинтересовать воров.
* Подросток может спровоцировать травлю себя со стороны пользователей сети.
* Также через социальные сети возможно заражение его компьютера.

Стоит отдельно рассказать про взлом профайла, и о том, как злоумышленники получают доступ к аккаунту. Вот некоторые самые популярные методы получения пароля:

* Метод обмана – очень распространенный метод доступа к личным данным. Сюда входят различие предложения, которые кажутся очень интересными.
* Программные методы. Этот метод взлома доступен знающим людям и состоит в поиске ошибок в коде сайтов, позволяющих получить доступ к базе данных с паролями. В таком случае данные могут восстановить только администраторы.
* Получить доступ к профайлу можно через отсылку письма с просьбой перейти по ссылке и там ввести свои данные, или просто выслать свои данные для перерегистрации, представляясь сотрудниками портала. Вариантов много, а цель одна – через письмо человек вводит свой пароль, а злоумышленники его получают. В этом случае пользователь практически безвозвратно теряет свою почту и все свои аккаунты, зарегистрированные на нее.
* В интернет-кафе, а также у друзей, которые хотели бы получить чужой пароль. Киберпреступники могут использовать программы, называемые KeyLogger-ами – это клавиатурные шпионы, перехватывающие нажатия на клавиатуру и записывающие их в файл, таким образом, злоумышленник сможет получить любой пароль. Такая программа может быть установлена на любом общественном компьютере, в том числе в интернет-кафе.
* Путем прямого контакта с жертвой и выяснения, что может быть паролем. Метод очень опасен для подростка, если применяется опытным человеком. Не надо никому сообщать свои личные данные, даже если этот человек будет представляться сотрудником техподдержки или администрации.
* Посредством перебора пароля по словарю или ручного подбора самых часто используемых простых паролей.
  + - Предложениями скачать всевозможные программы, на самом деле являющиеся опасными вирусами, которые не всегда сразу определяются антивирусами, загрузить фото вместо граффити, установить новые смайлики, отправить cookies, логин и пароль в адрес неких людей, которые представляются сотрудниками техподдержки или администрации.
* Взлом твоего компьютера, где киберпреступники находят пароли. Это очень сложный способ и очень часто антивирусные программы замечают подобную деятельность. Обычно используются троянские программы.

**Правила безопасного поведения в социальных сетях**

Тонны сокровенных подробностей, о которых сказать незнакомому человеку на улице даже в голову не придёт, выкладываются в социальные сети, где к этим деталям личной жизни потенциально имеют доступ миллионы незнакомых людей. «Чепуха! Очередная паранойя. Я могу себя чувствовать уютно и в безопасности в кругу своих друзей, т.к. безупречная настройка приватности меня защитит» - то о чём, скорее всего, Вы подумали сейчас.

Только проблема в том, что своей личной жизнью мы делимся не лично с человеком, а с его аккаунтом... Наивно полагать, что его аккаунт полностью защищён. Он может быть взломан.

А возможно, ваш друг не сильно заботится о конфиденциальности своего общения в сети и у него все время активно подключение к социальным сетям или включено автозаполнение паролей, дабы экономить время, а вход в операционную систему без пароля. Чем и не преминул воспользоваться только что вышедший на волю жуткий троюродный брат по двоюродной тётке вашего друга, зашедший к нему в гости.

Многие люди любят оповещать о своём местонахождении в социальных сетях. Особенно, если в этом месте потрясающая архитектура или песок, солнце и океан. Тем, кто имеет доступ к вашей странице не нужно знать, где Вы находитесь в режиме 24/7.

Касательно вашего месторасположения нужно использовать только прошедшее время, а не настоящее и будущее. Не размещайте в социальных сетях ту информацию, разглашение которой нежелательно для Вас, даже если Вы на сто процентов уверенны, что она будет доступна только определённым людям.

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация размещенная в интернете может серьезным образом отразиться на твоей реальной жизни.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.

Цифровая репутация» - это твой имидж, который формируется из информации о тебе в интернете. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети.

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающее люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

В мире цифровых технологий может быть непросто сформировать свой новый образ. Даже если ты не хочешь, чтобы о твоих старых приятелях стало известно, эта информация остается в Интернете, и любой сможет ее найти. Свидетельства неприличного поведения тоже будет невозможно скрыть.

То, что когда-то казалось подходящим для публикации, в один прекрасный день может всплыть на поверхности и причинить тебе различные неприятности.

Если ты хочешь узнать, что о тебе можно узнать, то набери свое имя и фамилию в поисковую систему и посмотри, какая информация выдается. Если что-то тебе не понравится, то постарайся удалить это.

Но у всего есть и хорошая сторона. Если ты формируешь свой положительный образ, то ты делаешь все правильно. Например, это может быть размещение информации об участии в каком-то конкурсе, ссылка на твою статью в школьной газете или просто грамота. Также это позволяет продемонстрировать сферу твоих достижений, что пригодится в будущем при обучении и продвижении по карьерной лестнице, а также позволит установить связи с людьми, имеющими схожие интересы. Важно, что это должно быть правдой.

Около 85% сотрудников отделов кадров говорят, что учитывают цифровую репутацию, решая, принять ли человека на работу. Поэтому твоя цифровая репутация очень важна, а думать над этим лучше уже сейчас.

Одна из опасностей социальных сетей-секстинг. Это пересылка личных фотографий, сообщений интимного содержания посредством современных средств связи: сотовых телефонов, электронной почты, социальных интернет-сетей.

Обычно наши ровесники используют камеры, встроенные в мобильные телефоны, чтобы сфотографировать себя в обнаженном или полуобнаженном виде и отправить эти картинки своим друзьям, подругам или одноклассникам. Некоторые отправляют эти фотографии только одному человеку, а уже тот в свою очередь пересылает их другим людям.

Секстинг выглядит как забава или какая-то игра до тех пор, пока кто-нибудь не пострадает, а скорее всего, пострадаешь именно ты. Проблема секстинга заключается в том, что конфиденциальные фотки могут быстро стать достоянием общественности. Смелая фотка, отправленная сегодня твоему другу или подруге, завтра может начать бесконтрольно распространяться, в результате чего автор станет посмешищем в школе, на него выльется много грязи и сплетен. Когда фотография становится доступной в Интернете, то практически невозможно удалить все ее копии.

В некоторых странах, в частности в Российской Федерации, секстинг является уголовным преступлением, а если на интимных фотографиях изображен несовершеннолетний, то это считается детской порнографией. Причём виновными могут быть признаны оба: как человек, отправивший фотографии, так и получивший их — это классифицируется как производство и хранение детской порнографии соответственно. Кроме того, лицу, пославшему свои фотографии в обнажённом виде, могут быть предъявлены обвинения в сексуальном домогательстве.

**Как помочь ребенку, если он уже столкнулся с Интернет-угрозой**

Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен Вам доверять и знать, что Вы хотите разобраться в ситуации и помочь ему, а не наказать.

Постарайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка.

Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети), или он попал в неприятную ситуацию (потратил Ваши или свои деньги в результате интернет-мошенничества и пр.) — постарайтесь его успокоить и вместе с ним разберитесь в ситуации — что привело к данному результату, какие неверные действия совершил сам ребенок, а где Вы не рассказали ему о правилах безопасности в Интернете.

Если ситуация связана с насилием в Интернете по отношению к ребенку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о встрече в реальной жизни; узнать были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т.п.), жестко настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время.

Соберите наиболее полную информацию о происшествии, как со слов ребенка, так и с помощью технических средств — зайдите на страницы сайта, где был Ваш ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию — в дальнейшем это может Вам пригодиться (например, для обращения в правоохранительные органы).

Если Вы не уверены в оценке серьезности произошедшего с Вашим ребенком, или ребенок недостаточно откровенен с Вами или вообще не готов идти на контакт, или Вы не знаете как поступить в той или иной ситуации — обратитесь к специалисту (телефон доверия, горячая линия и др.), где Вам дадут рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организаций (МВД, МЧС, Сестры и др.)

**Сервисы, позволяющие родителям контролировать использование Интернета детьми**

КиберМама™ http://www.cybermama.ru - программа для ограничения времени работы на компьютере детей и подростков. Позволяет создавать расписание работы ребенка за компьютером и автоматически контролировать нежелательных игр и программ, блокировать доступ в Интернет. Программа проста и понятна в использовании и не требует от родителей специальных компьютерных навыков и знаний.

NetKids - сервис, который позволяет родителям контролировать использование интернета детьми. NetKids это:

* блокировка доступа к опасным сайтам;
* отчеты о посещенных сайтах;
* мониторинг общения в социальных сетях;
* контроль загрузки фотографий и личной информации;
* отчеты о поисковых запросах;
* мониторинг почтовых сообщений и записей в блогах.

Вся работа осуществляется через удобный и понятный web-интерфейс.

KinderGate Родительский Контроль 1.0. Эта программа-фильтр (www.usergate.ru) предлагает 82 категории фильтрации веб-сайтов в 5 основных уровнях доступа (по умолчанию запрещен доступ к фишинговым ресурсам, сайтам с порнографическим контентам, а также к сайтам, содержащим вредоносный код). Самый высокий уровень фильтрации подразумевает, в числе прочего, запрет прокси-серверов, сайтов знакомств. Доступно создание расширенных правил, «черных» и «белых» списков для сайтов. Можно установить ограничение скачивания видео, звуковых файлов, изображений, архивов и EXE-файлов, документов. В программе реализован модуль морфологического анализа, позволяющий блокировать веб-страницы с нецензурной лексикой. Для ограничения времени, проводимого ребенком за компьютером, предусмотрен специальный инструмент «Расписание работы». Кроме этого, доступна статистика посещенных веб-ресурсов с указанием значений входящего и исходящего трафика, а также просмотр сообщений в сетях odnoklassniki.ru и vkontakte.ru. Интернет Цензор – интернет-фильтр, предназначенный для блокировки потенциально опасных для здоровья и психики подростка сайтов. В основе работы программы лежит технология «белых списков», гарантирующая 100%-ную защиту от опасных и нежелательных материалов. Фильтр «Интернет Цензор» можно скачать бесплатно на официальном сайте. Программа содержит уникальные вручную проверенные «белые списки», включающие все безопасные сайты Рунета и основные иностранные ресурсы. Программа надежно защищена от взлома и обхода фильтрации. «Интернет Цензор» может использоваться как в домашних условиях, так и в образовательных учреждениях, библиотеках, музеях, интернет-кафе и иных местах, где возможно предоставление несовершеннолетним доступа в Интернет.

**Полезные сайты для родителей**

http://www.nachalka.com/bezopasnost – Безопасность детей в Интернете

http://www.ifap.ru/library/book099.pdf – Безопасность детей в Интернете

http://www.microsoft.com/ru-ru/security/default.aspx – Центр безопасности Microsoft

http://www.fid.su/projects/journal/ – Фонд развития Интернет. Журнал «Дети в информационном обществе»

http://www.friendlyrunet.ru/safety/74/index.phtml – Фонд «Дружественный Рунет»

http://netpolice.ru/filters/ – Фильтры NetPolice

http://www.socobraz.ru/index.php/Сообщество\_родителей – Сообщество родителей СОЦОБРАЗ

http://www.microsoft.com/ru-ru/security/family-safety/kids-social.aspx – Как помочь вашим детям более безопасно пользоваться сайтами социальных сетей?

http://windows.microsoft.com/ru-RU/windows7/products/features/parental-controls – Родительский контроль в Windows 7

http://play.mirchar.ru/sovety-roditelyam-po-obespecheniyu-bezopasnosti-detey.html – Консультации для родителей по обеспечению безопасности детей в Интернет

http://www.internet-kontrol.ru/ –Защита детей от вредной информации в сети Интернет

http://www.oszone.net/6213/ – Обеспечение безопасности детей при работе в Интернет

http://wiki.saripkro.ru/index.php/Интернет-безопасность\_для\_родителей – Интернет-безопасность для родителей

http://www.sch169.ru/doc/pam.pdf – Как защититься от интернет-угроз

**Памятка по технике безопасности в социальных сетях**

* Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей.
* Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
* Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
* Используй настройки конфиденциальности аккаунта. Настрой просмотр содержимого твоей учетной записи "только для друзей”. Таким образом, незнакомые люди не увидят твою личную информацию;
* Принимай запросы в друзья только от тех людей, которых ты знаешь и которым доверяешь;
* Не используй веб-камеру для общения с людьми, которых ты не знаешь;
* Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
* Будь осторожен - некоторые пользователи могут представляться кем угодно;
* Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
* При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
* Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу;
* Не размещай фотографии и видео со своими друзьями без их разрешения. Обращайся к друзьям, чтобы они также соблюдали конфиденциальность и не размещали твои фотографии и видео в общем доступе;
* Никогда не открывай подозрительные ссылки, даже если они пришли от твоих друзей. Удостоверься в том, что друг тебе выслал эту ссылку сам, а его аккаунт не контролирует киберпреступник. После взлома аккаунта злоумышленники в первую очередь делают рассылку по адресной книге, а поскольку доверие друзей друг другу выше, то вероятность заражения вирусами резко вырастает;
* Чтобы попасть в свою социальную сеть или на какой-либо другой сайт лучше используй закладки или окно быстрого доступа. Таким образом, ты точно попадешь на те порталы, которые безопасны и которыми ты пользуешься. При наборе адреса есть риск того, что ты ошибешься с адресом и не заметишь этого.