

Тема: «Кибербезопасность в подростковой среде»

Автор:

Корабовцева Светлана Александровна

МОУ СОШ №8 г.Каменки, 11 класс

Научный руководитель:

Царапкина Юлия Михайловна

Кандидат педагогических наук,

доцент кафедры педагогики и психологии профессионального образования

РГАУ – МСХА имени К.А.Тимирязева

2023г.

Пензенская область, г.Каменка

Оглавление

Введение	3
1.Обзор литературы	
1.1 Возможности интернета и социальных сетей	6
1.2 Коммуникационные риски общения в социальных сетях	7
1.3 Информация нежелательного характера. Контентные риски	8
1.4 Опасные интернет – сообщества	9
1.5 Фейк в интернете	9
1.6 Законодательство в сфере кибербезопасности	10
2.Методы исследований	12
3.Результаты и обсуждения	
3.1 Результаты собственного исследования	13
3.2 Результаты исследования «Лаборатории Касперского»	16
4.Выводы	17
5.Список литературы	17
Приложения	18

ВВЕДЕНИЕ

Одной из характерных особенностей нашего времени является быстрое развитие средств массовой коммуникации.

Многие поколения наших предков пользовались единственным средством накопления, хранения и передачи информации - устным словом. С появлением бумаги, изобретением наборного шрифта и печатного станка, а затем типографской машины, распространение печатного слова приобрело массовый характер. С возникновением в 20 веке электронных средств связи характер СМИ - а фактически жизни в целом - изменился коренным образом. Немалую роль здесь играет такое явление, как глобальная сеть Интернет.

Интернет – величайшее и удивительное изобретение прошлого столетия, при помощи которого человечество совершило огромный скачок в будущее, дало стимул к прогрессу. Интернет упрощает нашу жизнь, открывает перед нами большие возможности! Современный человек постоянно сталкивается с использованием интернета для решения повседневных задач: для учебы, творчества, профессиональной деятельности и т.д.

В любое время общение – наиважнейший способ взаимодействия между людьми. Современным средствам коммуникации под силу преодоление расстояний, времени, социальных барьеров, личностных проблем в общении.

Обмен сообщениями происходит мгновенно, можно обмениваться не только текстовой информацией, но и мультимедийным контентом. Можно общаться с родственниками и знакомыми, живущими очень далеко, быстро узнавать новости о жизни, успехах и неудачах разных людей, следить за их творчеством – это только небольшой перечень тех возможностей, которые использует пользователь сети интернет.

Однако, существует и много негативных факторов, которые делают сетевое общение неприятным, несут угрозу психологическому здоровью, финансовому состоянию.

Самой уязвимой аудиторией в этом поле оказываются дети, которые не склонны видеть подвоха там, где всё «естественно»: беседа, игра, обмен подарками или фото, видеороликами и аудиозаписями; где все твои интересы на виду, равно как и интересы твоих собеседников; где нет видимой физической опасности. Если младшие школьники как то находятся под контролем родителей, то более самостоятельные - подростки - слишком много времени уделяют общению в социальных сетях, онлайн-играм и интернету в целом. Именно они оказываются первыми в группе «риска» среди пользователей интернета, так как не умеют правильно оценивать безопасность информационного контента в социальных сетях.

Подростки в интернете сталкиваются с теми же рисками, что встречаются им в обществе . В реальной жизни угрозы достаточно локализованы – они могут исходить от родственников, сверстников, учителей, представителей социальных служб, знакомых из ближайшего окружения. В сетевом же пространстве угрозы могут исходить от кого угодно и откуда угодно – без географической или какой-то другой привязки.

Известно, что подростковый возраст - самый опасный период в формировании зависимого поведения. Для этого возраста характерно стремление к познанию всего нового, необычного, «чувство взрослости», которое выражается в гипертрофированной потребности самостоятельности, самоутверждения, отказ от детской «морали успеха», желание копировать привычки и способы поведения старших, боязнь отстать от сверстников, казаться в их глазах смешным.

Возрастные особенности подростков характеризуются негативизмом, как крайним проявлением реакции эмансипации. Основную причину, которая погружает молодого человека в мир виртуальных событий, зарубежные исследователи видят в коммуникативной депривации, то есть ребенок становится закрытым для откровенного общения со сверстниками. Кроме того, он теряет эмоциональный контакт с родителями или педагогами.

Наблюдая за школьниками, которые меня окружают, я заметила, что все подростки активно используют интернет, социальные сети в своей повседневной жизни. Возрастные ограничения доступа для большинства ребят не представляют препятствия для регистрации и использования сети, с одобрения родителей, которые не оценивают всей опасности свободного доступа ребенка к интернету, персональные данные меняются, и ребенок отправляется в «свободное плавание» по интернету. Проблема состоит в том, что не все юные пользователи знают об опасностях сети интернет, а сталкиваясь с проявлением интернет-преступлений, не всегда могут себя защитить.

Участившиеся по всей России случаи киберпреступлений в отношении детей говорят о необходимости целенаправленного формирования у них навыков безопасной работы в киберпространстве.

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

Это определило цель моего исследования: выявить основные риски взаимодействия подростков в социальных сетях.

Задачи проекта:

1. Показать актуальность данной темы;
2. Изучить и проанализировать самые распространенные контентные риски;
3. Познакомиться с нормативно – правовыми актами, регулирующие основы безопасности Интернета и защиту ребенка в киберпространстве;
4. Выявить уровень знаний по кибербезопасности учащихся 9-11 классов;
5. Разработать информационные буклеты по кибербезопасности и распространить их среди учащихся нашей школы.

Объект исследования: взаимодействие подростков в социальных сетях.

Предмет исследования: негативные факторы сети интернет.

Способы достижения цели:

1. Изучение научно–популярного материала по данной теме;
2. Анализ и синтез полученной информации;
3. Анкетирование, наблюдение.
4. Анализ полученных данных анкетирования и наблюдения.

Гипотеза исследования: сеть интернет скрывает большое количество контентных рисков, но если знакомить учащихся с правилами безопасности в сети интернет начиная с начальной школы, то в более старшем возрасте их сетевое общение станет более безопасным.

1.ОБЗОР ЛИТЕРАТУРЫ

1.1 Возможности интернета и социальных сетей.

По последнему отчету Global Digital за 2023г. сегодня в мире насчитывается 5,16 миллиарда пользователей интернета. Это значит, что 64,4% мирового населения имеют доступ в интернет. За год количество интернет - пользователей выросло на 1,9%.

Россия занимает первое место в Европе по количеству пользователей Интернета и шестое место в мире. Уровень проникновения интернета в России — 89 %, а это 129,8 из 145,9 миллионов человек, причем дети и несовершеннолетние составляют 21,8 % от населения страны. За 2021 год количество пользователей интернета увеличилось на 4,7 %.

Социальная сеть — это интернет-площадка, сайт, который позволяет зарегистрированным на нем пользователям размещать информацию о себе и коммуницировать между собой, устанавливая социальные связи. Контент на этой площадке создается непосредственно самими пользователями. Социальные сети являются одним из востребованных интернет-сервисов для всех поколений пользователей.

Первая социальная сеть появилась в 1995 году на котором можно было найти своих одноклассников, однокурсников, друзей.

Самые популярные сети на сегодняшний момент среди подростков – Вконтакте, TikTok.

В социальных сетях можно:

- смотреть новости.;
- публиковать информацию о себе или любой другой контент;
- общаться с друзьями, знакомиться⁴
- комментировать публикации других пользователей;
- вступать в тематические сообщества;
- слушать музыку, смотреть видео;
- делать покупки;
- играть в игры.

Сейчас социальные сети — это не только площадки для развлечения и общения. Это также рекламные площадки.

Интернет к сегодняшнему дню стал некой параллельной реальностью. Так что все виды мошенничества, которые существуют в реальном мире, все это есть и в интернете. Только там никто практически не контролирует все это движение.

С каждым днем появляются новые механики, представляющие угрозу для детей и подростков в интернете. Чтобы создать безопасность интернета для детей, нужно знать чем он опасен.

1.2 Коммуникационные риски общения в социальных сетях.

Кибербуллинг – преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство та же травля, которая существует и в реальном мире.

Ребенок может быть не только жертвой, но и активным участником кибербуллинга, даже если в обычной жизни он не конфликтен. Интернет становится для многих своеобразным «Бойцовским клубом», но кибербуллинг может быть столь же опасным и болезненным, как и реальная травля: 13% онлайн-конфликтов перерастают в самые настоящие столкновения в реальной жизни, а около 7% подвергшихся травле детей получают такие психологические травмы, что не могут оправиться по полгода.

Троллинг – намеренная провокация про помощи оскорблений или некорректной лексики на интернет – форумах и в социальных сетях. Тролли будут лично нападать на жертву и стараться унижить ее. Основная задача троллинга – разозлить жертву и заставить ее прибегнуть, так же как и сам тролль, к оскорблениям и некорректной лексике. Тролли могут тратить долгое время в поисках особенно уязвимой жертвы. Как правило, тролли получают положительные эмоции за счет унижения других.

Груминг в интернете — это ситуация, в которой опасный незнакомец втирается в доверие к ребенку, устанавливает с ним тесный эмоциональный контакт для дальнейшей сексуальной эксплуатации.

Секстинг — явление, тесно связанное с грумингом, — представляет собой обмен откровенными сообщениями и интимными снимками, иными словами, это сексуальная эксплуатация непосредственно в онлайн-пространстве.

Вишинг – назван по аналогии с фишингом- распространенным сетевым мошенничеством. Сходство названий подчеркивает тот факт, что принципиальной разницы между фишингом и вишингом нет. Основное отличие вишинга в том, что так или иначе задействуется телефоном. Типичный пример фишинга, когда клиенты какой-либо платежной системы получают сообщения по электронной почте якобы от администрации или службы безопасности данной системы с просьбой указать свои счета, пароли и т.п. При этом ссылка в сообщении ведет на поддельный сайт, на котором и происходит кража информации. Сайт этот уничтожается через некоторое время, и отследить его создателей в интернете достаточно сложно.

1.3 Информация нежелательного характера. Контентные риски.

К противозаконной и вредоносной информации относятся:

- пропаганда насилия, жестокости и агрессии;
- пропаганда и распространение наркотических и отравляющих веществ;
- пропаганда азартных игр;
- разжигание расовой ненависти, нетерпимости по отношению к другим людям по национальным, социальным, групповым признакам;

- пропаганда деятельности различных сект, неформальных молодежных движений;
- нецензурная лексика и т.д.

В сети Интернет такую информацию можно встретить практически везде: в социальных сетях, блогах, персональных сайтах, видеохостингах и др. Не являются исключением и мобильные сервисы.

1.4 Опасные интернет – сообщества.

В 2015 году в социальных сетях стали массово появляться группы, где детей склоняют к суициду в режиме онлайн. В них детей заставляют покончить собой, транслируя видео этого в сети Интернет. По мнению в правоохранительных органов в таких группах работают профессиональные психологи, которые методично доводят детей и подростков до самоубийства. Модераторы групп смерти часто сами находят подростков, которые уже и так страдают от депрессии и не скрывают своих суицидальных мыслей.

Есть сообщества, где принято хвастаться своей худобой. Девочки – подростки ненавидят свое тело, стремятся к идеалу. Подростков подсаживают на различные диеты и пропагандируют свой образ жизни. Тем самым количество их быстро растёт. Для них это, как наркотик, который также может привести к смерти.

Группы по вербовки в запрещенные организации и группы.

В интернете действует сеть по вербовке в международные террористические организации. Национальность и вероисповедание для этих людей не играет роли.

1.5 Фейк в интернете.

Фейк – это фальшивка, подделка: новость, которая неправдоподобна; аккаунт человека в соцсети, которого на самом деле не существует; смонтированный видеоролик и т.п. На самом примитивном бытовом уровне встречаются фейки-подделки известных брендов, производящих фирменную одежду, обувь и другую продукцию. Созвучное название, где изменена всего одна буква, вводит потребителя в заблуждения, заставляя принимать подделку за товар надежного производителя.

Цель производителей подобной продукции очень проста. Получение прибыли, которая возникает за счет роста продаж поддельной продукции, принимаемой покупателем по ошибке за известную марку.

1.6 Законодательство в сфере кибербезопасности.

Законодательство РФ предусматривает наказание за киберпреступления.

Статья 272. Неправомерный доступ к компьютерной информации наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

УК РФ, Статья 273. Создание, использование и распространение вредоносных компьютерных программ. Наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

УК РФ, Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

Законодательство РФ предусматривает защиту и безопасность подрастающего поколения.

В 2010 году была подписана Декларация «За безопасность детей и молодежи в Интернете».

В Декларации были определены главные направления деятельности по защите от информации, причиняющей вред здоровью и развитию детей: создание и поддержание условий конструктивного и развивающего взаимодействия детей и молодежи с Интернетом; снижение и предотвращение рисков, связанных с возможностью контакта несовершеннолетних с потенциально опасным и противоправным интернет-контентом, а также с лицами, использующими Интернет с целью шантажа, преследования, совращения, сексуальной эксплуатации и с другими противоправными намерениями.

21 июля 2011 года был подписан Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию».

Принятие данного Федерального закона направлено «на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребёнке порочные склонности, сформировать у ребёнка искажённую картину мира и неправильные жизненные установки» [Федеральный закон..., 2011].

В Федеральном законе Российской Федерации от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации», подписанном 28.07.2012 г. в Статье 15 определён единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.

Начиная с 2010 года, в России проводятся ежегодные Форумы безопасного Интернета, на которых обсуждаются актуальные проблемы обеспечения безопасности подрастающего поколения в медиапространстве.

Результаты исследовательской и практической деятельности по обеспечению безопасности детей в Интернете публикуются на портале Года Безопасного Интернета (www.saferinternet.ru), сайте Форума Безопасного Интернета (www.safor.ru). Регулярно выпускаются информационные тематические публикации в электронных и печатных СМИ; издается информационно-аналитический журнал «Дети в информационном обществе».

2. МЕТОДЫ ИССЛЕДОВАНИЙ

Наблюдение за учащимися на уроках, переменах, в свободное от занятий время, с целью необходимости использования ими интернета.

2.2 Анкетирование.

Я провела анкетирование среди учащихся своей школы. Приняли участие 72 человека (учащиеся 10-11 классов).

1. Сколько времени ты тратишь в интернете?

- | | |
|----------------------------|----------------------------|
| а. Всё свободное время, | г. До 1-ого часа в день, |
| б. Несколько часов в день, | д. Несколько раз в неделю, |
| в. До 3-х часов в день, | е. Несколько раз в месяц |

2. Для каких целей используется интернет?

- | | |
|------------------|---------------------------------|
| а. Для учебы, | г. Поиск какой либо информации, |
| б. Для общения, | д. Другое. |
| в. Он-лайн игры, | |

3. Зарегистрированы ли вы в каких либо сетях?

4. Как ты считаешь, опасен ли интернет?

- | | |
|-------------------|---------------|
| а. Опасен, | в. Не опасен, |
| б. Опасен иногда, | г. Не знаю. |

5. Знаете ли Вы, какие угрозы существуют в Интернет-пространстве?

(перечислите их)

По данным опроса выяснилось, что подростки имеют представление о существовании угроз в Интернет-пространстве. Наиболее часто были отмечены: утечка личной информации и персональных данных (31%), мошенничество (26%), кибербуллинг, фишинг (24%),

Взлом аккаунтов в социальных сетях(20%); Вредоносные программы, вирусы(18%);Шантаж, вымогательство(5%).6.Как ты реагируешь на получение спамов, рекламных роликов, различных сообщений, содержащих неприятную информацию, оскорбление, запугивание и т.д.

7.При регистрации в социальных сетях ты пользуешься настоящим или вымышленным именем?

8.Делишься ли ты с малознакомыми людьми в Интернете личной информацией?

9.Твоя реакция на предложение добавить «нового друга»?

10.Делитесь ли вы с друзьями в социальной сети информацией, разглашения которой вы бы не хотели?

а) да б) нет в) не помню.

11.Размещаете ли вы в социальных сетях личную информацию: номер домашнего телефона, номер школы и класса, свои личные данные и фотографии?

а)да б) нет в) не помню.

12.Вступаете ли вы в социальных сетях в переписку с незнакомыми людьми? а) да б) нет

13.Случалось ли вам обмениваться фотографиями с незнакомыми людьми в социальных сетях? а)да б) нет

14.Сталкивались ли вы когда-нибудь с проблемами, связанными с использованием социальных сетей? а) да б) нет

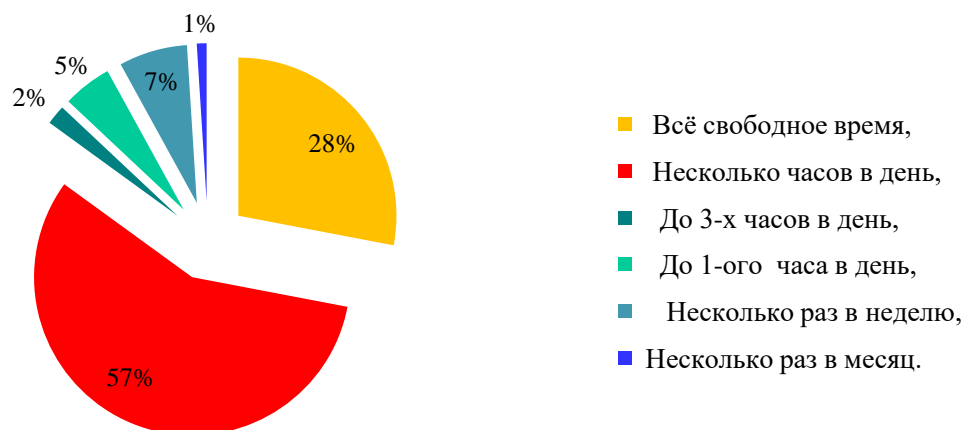
3. РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЯ

3.1 Результаты собственного исследования.

Проведя наблюдение и анкетирования получились следующие результаты.

Учащиеся очень много времени проводят в Интернете, по несколько часов в день (57%). Из наблюдений было выявлено, что даже во время уроков, на перемене выходят в сеть Интернет по вопросам, не касающимся учебной деятельности.

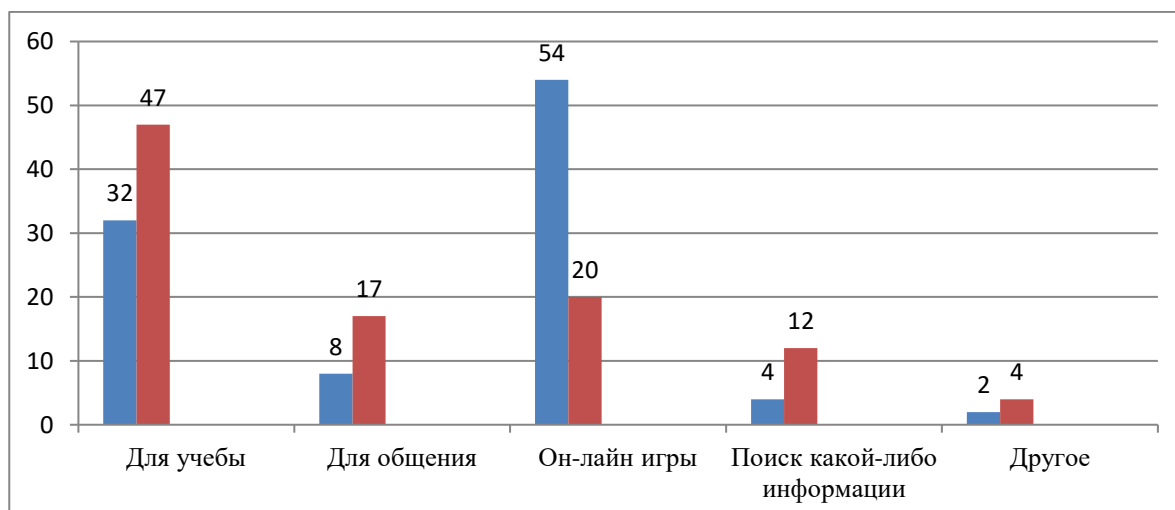
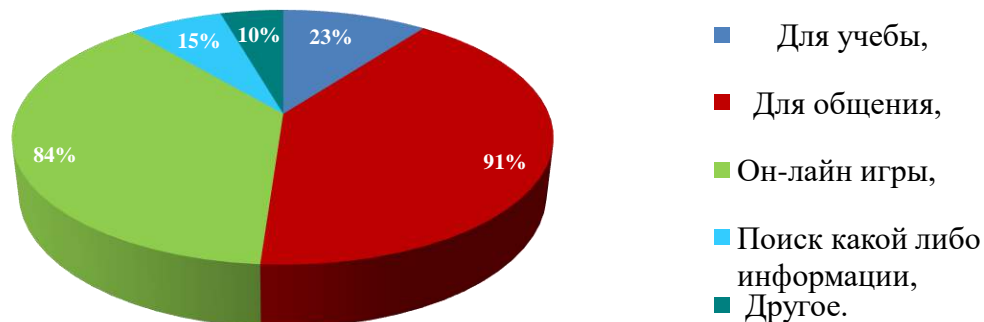
Время проведения учащимися сети интернет



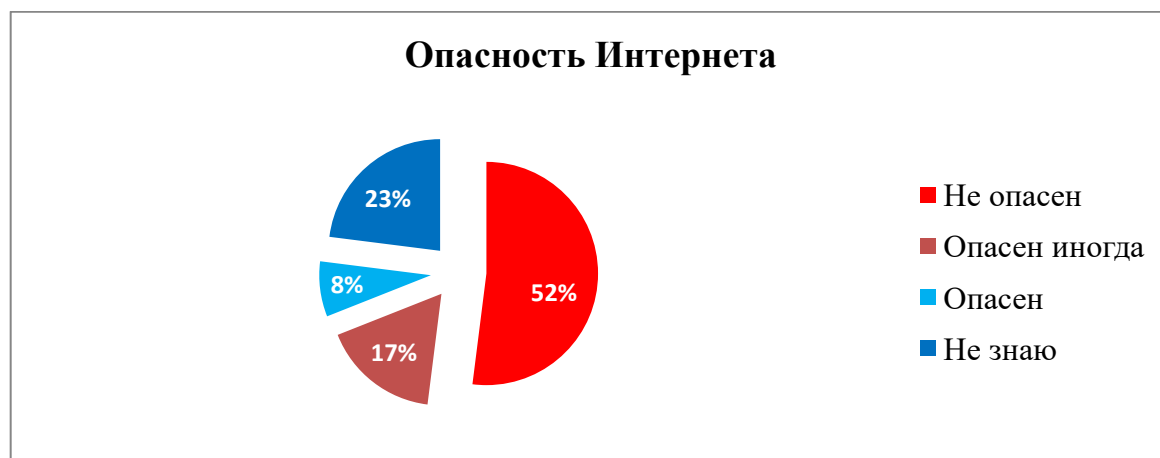
Причем девочки больше времени уделяют времени Интернет, чем мальчики.

Ответ на вопрос : с какой целью используется интернет, показал, что учащиеся используют интернет в большей степени для общения (91%) и для игр (84%), причем мальчики для игр, а девочки для общения.

Цели использования Интернет

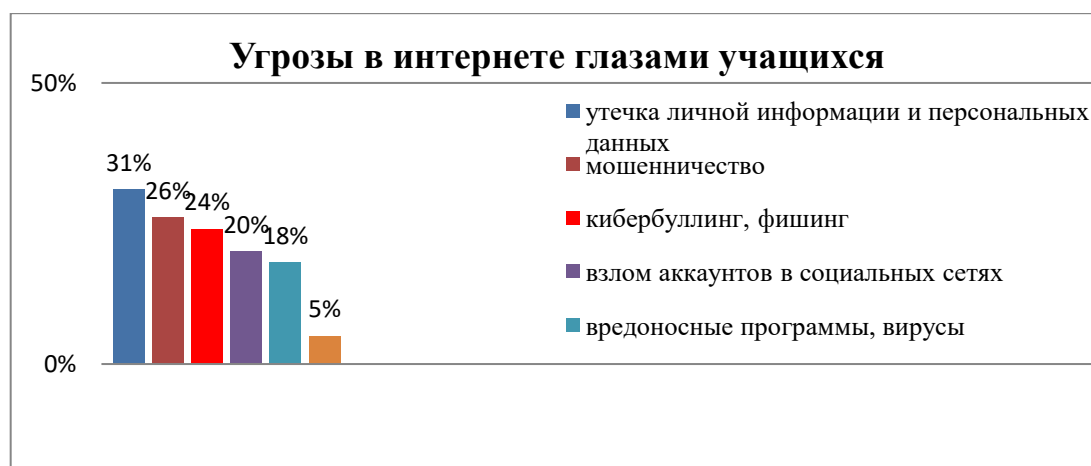


По результатам опроса было выявлено 52% считают, что интернет не опасен, 23 % не смогли точно ответить на вопрос, 17% ответили, что интернет не всегда опасен, и только 8% ответили, что интернет опасен.



Было выявлено, что из-за постоянного пребывания в Интернете у опрошенных учащихся появились проблемы со здоровьем: нарушилась осанка, испортилось зрение, появились головные боли.

По данным вопроса «Знаете ли Вы, какие угрозы существуют в Интернет-пространстве?» выяснилось, что подростки имеют представление о существовании угроз в Интернет-пространстве. Наиболее часто были отмечены: утечка личной информации и персональных данных (31%); мошенничество (26%); кибербуллинг, фишинг (24%); взлом аккаунтов в социальных сетях (20%); вредоносные программы, вирусы (18%); шантаж, вымогательство (5%).



Это самые распространённые угрозы, которые известны подросткам.

Про другие мало кто слышал или совсем не имеют представления.

Подавляющее большинство 95% подростков зарегистрированы в социальных сетях и поддерживают активные контакты с малознакомыми или незнакомыми людьми 34%.

При регистрации в социальных сетях 85% учащихся пользуются настоящим именем. 23% делятся в Интернете с малознакомыми людьми личной информацией.

3.2 Результаты исследования «Лаборатории Касперского».

В 2021 г. по заказу «Лаборатории Касперского» опросили 500 респондентов. 82% несовершеннолетних участников исследования заявили, что получали заявки на добавление в друзья от незнакомых людей в социальных сетях, 50% детей знакомились в соцсетях и 37% детей встречались в реальной жизни с теми, с кем познакомились в соцсетях.

Согласно исследованию, у каждого четвертого ребенка информация в профиле доступна всем. Чаще всего дети (51%) в сети рассказывают о своих увлечениях и хобби, 27% отмечают номер школы, 13% выкладывают фотографии, где видно обстановку квартиры, 12% указывают имена родственников, 10% публикуют номер мобильного телефона.

Онлайн-опрос подростков «Оценка реакции подростков на вредоносное содержание в сети Интернет» показали следующие результаты: 41 % опрошенных подростков удаляют эту информацию, если они ее разместили; 32 % — пишут администратору сайта/группы/портала; 17 % — информируют родителей; 4 % — сообщают в полицию; 3 % — сообщают учителю; 22 % — не делают ничего.

Подростки недооценивают и игнорируют опасности, которые могут угрожать им при взаимодействии в социальных сетях;

4. ВЫВОДЫ

В своей исследовательской работе я постаралась выполнить все поставленные перед собой задачи. В ходе исследования я с помощью интернет-ресурсов разобралась, с какими угрозами подростки могут столкнуться и какие могут создать сами в интернет-пространстве. Также я нашла способы защиты данных и разработала рекомендации и буклет по защите подростков от интернет-угроз (Приложения). С помощью анкетирования я определила степень знаний подростков об интернет-угрозах.

На основании проведенного мной исследования, можно сделать следующие выводы. Гипотеза исследования подтвердилась. Мне удалось доказать на примере подростков, обучающихся в моей школе, что уровень их знаний и уровень осознанности интернет-угроз недостаточно высок.

В процессе работы над исследованием я приобрела опыт в безопасном использовании Интернета. Думаю, что полученные мной знания позволят избежать угроз, возможных при дальнейшем пользовании интернет-пространством не только мне, но и другим подросткам.

СПИСОК ЛИТЕРАТУРЫ

- 1.Безопасность в социальных сетях [Электронный ресурс]. – Режим доступа: http://welcom-comp.ru/antivir_pc/27-bezopasnost-v-socialnyh-setyah.html.
- 2.Алиева С.И. Киберпреступность: бич современного общества /С.И.Алиева//Оригинальные исследования. — Казань, 2021. — Т.11- № 4. — С. 213–218.
- 3.Калинина Н.В. Профилактика рисков интернет-активности обучающихся: субъект-порождающее взаимодействие. // Образование личности. – 2017- № 1. – с.12-17.
- 4.Не запрещать, а научить – безопасность подростков в социальных сетях [Эл. ресурс]–Режим доступа: <http://itworked.com.ua/article/view/bezopasnost-podrostkov-v-socialnyh-setyah/>.
- 5.Сохань С. И. Право несовершеннолетнего ребёнка на кибербезопасность /С. И. Сохань// Студенческий вестник. — Оренбург, 2019. — № 19–2. — С. 84–87.

ПРИЛОЖЕНИЯ

Приложение 1

Основные советы по 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;

Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;

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.

Приложение 2

Основные советы по борьбе с кибербуллингом:

Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;

Управляй своей киберрепутацией;

Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;

Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;

Веди себя вежливо;

Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;

Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Приложение 3

Основные советы по борьбе с фишингом:

Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;

Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;

Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;

Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;

Установи надежный пароль (PIN) на мобильный телефон;

Отключи сохранение пароля в браузере;

Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Рекомендации для родителя.

1. Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете, – правда.

2. Необходимо проверять информацию, увиденную в Интернете. Для этого существуют определенные правила проверки достоверности информации. Признаки надежного сайта, информации которого можно доверять, включают: авторство сайта, контактные данные авторов, источники информации, аккуратность в оформлении информации, актуальность данных.

3. Помните, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог – гораздо конструктивнее, чем постоянное отслеживание посещаемых сайтов и блокировка контента.

4. Обратите внимание на психологические особенности вашего ребенка. Признаки того, что ребенок подвергается кибербуллингу, – различны, но есть несколько общих моментов: видимый эмоциональный стресс во время и после использования Интернета, прекращение общения с друзьями, прогулы учебных занятий, нестабильные оценки, резкие перемены в настроении, поведении, склонность к депрессии.

5. Если у вас есть информация, что кто-то из друзей или знакомых вашего ребенка подвергается буллингу или кибербуллингу, то сообщите об этом классному руководителю или школьному психологу – необходимо принять меры по защите ребенка.

6. Выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаления странички.

7. Если поступающие угрозы являются достаточно серьезными, касаются жизни или здоровья ребенка, а также членов вашей семьи, то вы имеете право на защиту со стороны правоохранительных органов, а действия обидчиков могут попадать под статьи Уголовного и Административного кодексов о правонарушениях.