Муниципальное бюджетное
общеобразовательное учреждение
средняя общеобразовательная школа
сельского поселения «Поселок Тумнин»
Ванинского муниципального района
Хабаровского края

Безопасность в сети интернет.

Исследовательская работа по информатике

Выполнил: Михиенко Алексей,
Ученик 11 класса
Руководитель: Вракова Н.А.
учитель математики и информатики.

2022 год

Содержание

1.Введение

Мы живем в век информационных технологий. Компьютер, гаджет, интернет – эти понятия вошли в обиход нашей жизни, мы уже не можем жить без общения в сети. Через интернет осуществляется сейчас множество разных операций на рабочих местах в организациях, денежные операции при покупках в магазинах, за последние годы появилось большое количество интернет-сервисов различного направления: магазины, дизайн, обучение и т.д. Все вышеперечисленные факты говорят о том, что очень важным сейчас является грамотное, правильное, безопасное использование тех ресурсов, которые открывает интернет перед каждым пользователем.

Среди всех сетевых возможностей самым актуальным является общение по интернету, которое осуществляется через социальные сети и различные мессенджеры. Это удобно, т.к. 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. Первыми в группе «риска» среди пользователей интернета являются дети, т.к. они не умеют правильно оценивать безопасность информационного контента, но являются самыми активными в социальных сетях.

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.

Цель исследования в том, чтобы изучить самые распространенные контентные риски, сформулировать рекомендации, как избежать информации нежелательного характера, познакомить с этими материалами учеников нашей школы и их родителей, чтобы сделать их пребывание в интернете более безопасным.

Задачи проекта:

1. Изучить самые распространенные контентные риски;
2. Выявить уровень знаний по кибербезопасности учеников нашей школы;
3. Сформулировать рекомендации по кибербезопасности;
4. Провести тематическое занятие с учащимися начальной школы по безопасности в сети интернет;
5. Разработать информационные буклеты по кибербезопасности и распространить их среди учащихся нашей школы.

Объектом исследования являются негативные факторы сети интернет.

Методы исследования: изучение теоретического материала, анкетирование школьников, эксперимент по выявлению контентных рисков, проведение практического занятия.

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

Исследование интернет-рисков позволит систематизировать информацию о проблеме, подобрать информационные ресурсы по безопасности в сети интернет, созданные в ходе исследовательской работы буклеты можно тиражировать и распространять среди учащихся и их родителей.

2.Основная часть

2.1. Кибербезопасность.

По данным установочного исследования проекта WEB-Index, в феврале-ноябре 2020 года интернетом в России хотя бы раз в месяц пользовались в среднем 95,6 млн человек или 78,1% населения всей страны старше 12 лет. В среднем за день в интернет выходили 87,1 млн человек или 71,1% населения России. Проникновение интернета в России среди более молодого населения (до 44 лет) в 2020 году превысило 90%, а среди самых молодых россиян (12-24 лет) приблизилось к 100%. В группе населения 45-54 лет интернетом хотя бы раз в месяц пользовались 84,2% россиян, а среди самых старших жителей страны (55+ лет) в интернет выходит только половина – 49,7%.[1] В соответствии со статистическими данными, почти 100% россиян 12-24 лет ежедневно подвергаются опасности при неправильном пользовании интернетом.

Понятие кибербезопасности подразумевает под собой совокупность методов, технологий и процессов, предназначенных для защиты целостности сетей, программ и данных от цифровых атак. Целью кибератак является получение несанкционированного доступа к конфиденциальной информации, ее копирование, изменение или уничтожение. Так же могут служить для вымогательства денежных средств у пользователей или нарушения рабочих процессов в компании. Кибербезопасность может также упоминаться, как компьютерная безопасность или безопасность информационных технологий.

2.2. Коммуникационные риски общения в социальных сетях.

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 — портал Classmates.com, на котором можно было найти своих одноклассников, однокурсников или сослуживцев. Кстати, сеть существует и сегодня. Самые популярные сети на сегодняшний момент среди подростков – Вконтакте, TikTok.

Что можно делать в социальных сетях

- Смотреть новости.

- Публиковать информацию о себе или любой другой контент.
- Комментировать публикации других пользователей.
- Вступать в тематические паблики и сообщества.
- Общаться с друзьями, знакомиться.
- Заводить связи, искать работу или сотрудников.
- Слушать музыку, смотреть видео.
- Делать покупки. Некоторые соцсети интегрируют собственные платежные системы (например, VK Pay от «ВКонтакте»).
- Играть в игры.

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

- Рекламные площадки. Социальную сети активно используют рекламодатели, с помощью которой можно показывать рекламу тем, для кого она наиболее актуальна.
- Инструмент для продвижения личного бренда.
- Платформа для коммуникации брендов с целевой аудиторией. С помощью социальных сетей бренды повышают узнаваемость, информируют клиентов о различных изменениях. Общаются с клиентами и решают конфликтные ситуации (или не решают, если не умеют правильно отрабатывать негатив).
- Площадки для продажи товаров и услуг. Некоторые социальные сети предлагают инструменты для создания практически полноценных интернет-магазинов.
- Инструмент для формирования общественного мнения.

Социальные сети являются одним из инструментов сетевого общения. Это связано с определенными коммуникационными рисками. Примерами коммуникационных рисков могут служить знакомства в сети и встречи с интернет-знакомыми, интернет-хулиганство: преследование, запугивание и оскорбления, незаконные контакты и пр. С коммуникационными рисками можно столкнуться при общении в мобильных сервисах, чатах, онлайн-мессенджерах (Skype и др.), социальных сетях, на сайтах знакомств, форумах, блогах и т.д.

Виды рисков:

- **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.

- **Кибербуллинг** – преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство; социальное бойкотирование с помощью различных интернет – сервисов. Английское слово «буллинг» обозначает запугивание, унижение, травлю, физический или психологический террор, направленный на то, чтобы вызвать у других страх и тем самым подчинить его себе. Основной площадкой для кибербуллинга в последнее время являются социальные сети. В них можно оскорблять человека не только с помощью сообщений – нередки случаи, когда страницу жертвы взламывают (или создают поддельную на ее имя), где размещают лживый и унизительный контент.
- **Киберпреследование** – это преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет - коммуникаций. Также, киберпреследование может принимать также формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет – троллинг) и социальное бойкотирование.
- **Троллинг**– намеренная провокация про помощи оскорблений или некорректной лексики на интернет – форумах и в социальных сетях. Тролли будут лично нападать на жертву и стараться унизить 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.

2.3. Информация нежелательного характера. Контентные риски.

К противозаконной и вредоносной информации относятся:

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

Размещение противозаконной информации в сети Интернет преследуется по закону. Это относится в первую очередь к распространению наркотических веществ, призывам к разжиганию национальной розни и экстремистским действиям, особенно с участием несовершеннолетних.

Неэтичный, противоречащий принятым в обществе нормам морали и социальным нормам, контент не запрещен к распространению, но может содержать информацию, способную оскорбить пользователей и оказать вредоносное воздействие. Подобная информация не попадает под действие уголовного кодекса, но может оказать негативное влияние на психику человека, особенно ребенка. Примерами таких материалов могут служить широко распространенные в агрессивные онлайн-игры, азартные игры, информация о нездоровом образе жизни, принесении вреда здоровью и жизни, нецензурная брань, оскорбления и др. Неэтичная и вредоносная информация может быть направлена на манипулирование сознанием и действиями различных групп людей. Такая информация часто бывает заманчивой и оказывает сильное психологическое давление на детей и подростков, которые не способны до конца осознать смысл происходящего и отказаться от просмотра и изучения сайтов с негативным содержимым. Влияние подобного рода информации на еще неокрепшую психику детей и подростков – непредсказуемо; под воздействием таких сайтов может пострадать не только психика, но и физическое здоровье ребенка.

Вредоносный контент может привести к заражению компьютера вирусами и потере важных данных.

2.4. 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. Спортивная обувь “Adibas”, костюмы “Puna”, подделки продукции известных косметических брендов служат самыми типичными примерами товаров-фейков.

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

В интернет фейки запускаются со следующими целями:

- посещение чужих страниц и присутствие в соцсетях инкогнито;
- продвижение какого-либо товара или услуги в соцсетях, накрутка лайков, комментариев и т.п.;
- дезинформация, фальшивые новостные сообщения;
- фейковый профиль знаменитости для накрутки подписчиков;
- создание "видимости" движений на сайтах, в форумах, комментариях;
- мошенничество в Интернете: "липовая" продажа или покупка товаров и услуг;
- психологические проблемы создателей: представление себя как другого героя.

Особенности фейкового аккаунта:

- Существует недавно.
- Может прикрываться известной личностью.
- Анкета заполнена не полностью, нет индивидуальности.
- Странное имя (часто к нему добавляется продвигаемый товар или услуга).
- Мало фотографий.
- Спам на стене.
- Человек может редко заходить на страницу.

Для создания фейков в интернете есть множество причин, поэтому важно научиться отличать правду от вымысла. Имеет смысл проверять правильность ссылки, по которой предлагается пройти — некоторые из них очень похожи на адреса популярных сайтов. (Приложение 3).

2.5.Законодательство в сфере кибербезопасности.

Специалисты в области кибербезопасности работают в следующих структурах:

- отдел безопасности государственных структур, банковских и коммерческих организациях;
- правоохранительные органы;
- ИТ-компании;
- в компании занимающиеся производством и продажей компонентов и ЭВМ для защиты информации;
- службы организации защиты городской инфраструктуры.

Должность, которую могут занимать специалисты в области защиты информационных технологий:

- инженер-программист системы безопасности;
- специалист в области криптографии и стеганографии;
- консультант по развитию систем защиты в организации;
- инженер-исследователь систем технической безопасности;
- эксперт по компьютерной безопасности (тестировщик);
- инженер-проектировщик комплексных систем защиты;
- специалист по организации и управлению деятельностью службы безопасности;
- специалист в обеспечение банковской безопасности.

Честь, достоинство несовершеннолетнего гражданина охраняются теми же законами, что распространяются на лиц, достигших восемнадцатилетия. Оскорблением несовершеннолетнего считаются: насмешки, неэтичные замечания, обидные сравнения, нецензурные высказывания, неприличные жесты и предложения со стороны младших лиц, ровесников или совершеннолетних граждан, совершенные при личном общении пострадавшего и обвиняемой стороны, публично или с помощью возможностей интернета, либо мобильной связи.

Наказание за оскорбление несовершеннолетнего ребенка определяет суд.

Личное оскорбление – словесные обидные высказывания при личном общении.

Оскорбление на национальной, религиозной почве — унижение достоинства в связи с религиозными взглядами, поведением согласно традиций религии.

Оскорбление в социальной сети – размещение на страницах аккаунта пострадавшего, на страницах с общим доступом обидных высказываний, изображений с аморальным содержимым и пр.

Оскорбление несовершеннолетнего по телефону – систематическое высказывание грубостей, неэтичных замечаний с помощью возможностей стационарной или мобильной связи. Оскорбление ребенка ребенком. Прилюдное или при общении в личном формате, унижение достоинства ребенка другим ребенком в виде насмешек, обзывания, высмеивания внешнего вида, увлечений и пр.

За любой доказанный случай оскорбления назначается административное наказание. Какое наказание предусмотрено? Поскольку несовершеннолетние считаются лицами, не имеющими своего дохода, то административное наказание в виде штрафной санкции будут нести родители обвиняемого. Наказание для несовершеннолетнего, оскорбившего другого человека это административное – штраф.

3. Практическая часть

3.1. Анкетирование.

Изучая проблему нежелательного контента, я решил сделать провести практический эксперимент: насколько возможно подвергнуться риску при осуществлении поисковой деятельности в сети. Рассматривая теоретические аспекты проблемы исследования, я встретился со следующими рисками:

- окна всплывающей рекламы,
- ссылки с предложением перейти на другой сайт,
- предложения зарегистрироваться и ввести персональные данные,
- предложения сыграть в игру,
- информационные всплывающие сообщения о личной жизни артистов.

Среди моих знакомых есть пользователи, чьи аккаунты в социальных сетях были взломаны и использовались мошенниками для сбора денег и распространения нежелательной информации через сервис личных сообщений.

Можно сделать вывод, что при отсутствии знаний о киберугрозах пользователь (особенно в детском возрасте) может легко стать жертвой нежелательного контента или мошенников.

Я провел анкетирование среди учащихся своей школы. Приняли участие 48 человек. (Приложение 2,3)

Выводы:

1. Среди участников опроса большинство (65%) ответили, что проводят в Интернете большую часть своего свободного времени, примерно около 9 часов.
2. Все, кто проходил опрос, знают о киберугрозах.
3. Среди самых популярных ответов на вопрос «О каких киберугрозах ты знаешь?» равное количество ответов (по 36%)получили «Троллинг» и «Киберзапугивание».
4. С целью избежания киберугроз большинство респондентов (37%) предложили не размещать персональные данные в сети интернет.

3.2. Рекомендации по безопасности в сети Интернет

Рекомендации по предупреждению контентных рисков для подростков и их родителей.

На основе полученных данных мной разработаны рекомендации «Как избежать материалов с нежелательной информацией?»:

1. Установите на компьютер специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определенной тематикой.

2. Знайте, что у популярных поисковых систем и почтовых служб существуют специальные защитные функции, которые легко можно настроить самостоятельно.

3. Создайте на компьютере несколько учетных записей, чтобы каждый пользователь мог входить в компьютер (систему) независимо и иметь собственный уникальный профиль.

4. Поддерживайте доверительные отношения в семье, чтобы всегда быть в курсе, и родители знали, с какой информацией сталкиваешься ты в сети.

5. (для родителя) Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете, – правда. 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.

6.(для родителей) 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.

Рекомендации для родителей и детей по предотвращению интернет-хулиганства, кибербуллинга.

1.Подростки при общении в Интернете должны быть дружелюбными с другими пользователями. Ни в коем случае не надо писать резкие и оскорбительные слова – читать грубости так же неприятно, как и слышать.

2. Нужно правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же. Лучше вообще покинуть данный ресурс и удалить оттуда личную информацию, если не получается решить проблему мирным путем. Лучший способ испортить хулигану его выходку – полностью его игнорировать.

3. (Для родителей) 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.

4.(для родителей) 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.
5.Подростки, которые используют интернет, должны знать и понимать, что личная информация, которую они выкладывают в Интернете (домашний адрес, номер мобильного или домашнего телефона, адрес электронной почты, личные фотографии) может быть использована агрессорами против них. Обязательно нужно пользоваться настройками приватности.
6. Выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаления странички. Большинство социальных сетей и сервисов электронной почты имеют в настройках опцию «заблокировать пользователя» или «занести в черный список».
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.

Практическое занятие по безопасности в сети интернет с младшими школьниками.

Обучать правилам безопасности необходимо с младшего школьного возраста, когда ребенок только знакомится с возможностями сети интернет. Есть специальные сайты, где подобран материал для детей разного возраста по вопросам кибербезопасности. (Приложение 4)

Пользуясь доступным контентом, я подготовил и провел урок по безопасности в сети интернет в начальной школе.

4.Заключение

В ходе исследования мы выяснили, что большинство наших учащихся школы пользуются сетью интернет. Подготовленные рекомендации размещены на информационном стенде, учащиеся начальных классов получили буклеты. Родителям рекомендации разослали учителя нашей школы через мессенджеры. Теперь дети, подростки, родители знают рекомендации по предупреждению контентных рисков, по предотвращению интернет-хулиганства, кибербуллинга. Знают о том, что не нужно заходить на незнакомые нам сайты, скачивать неизвестные программы, размещать информацию о себе и своих близких. В случае, если все таки не удалось избежать неприятного случая, подросток будет знать, куда стоит обратиться за помощью.

С каждым годом тема кибербезопасности становится все более актуальной и необходимой в современном мире. Нам, пользователям сети Интернет, требуется сформировать эффективную политику безопасности информационных технологий, быть в курсе происходящего, т.е. следить за новостями в сфере защиты информации, а так же не забывать о том, что виртуальный мир, как и реальный - требует внимание к мелочам, даже к тем, который порой кажутся совсем незначительными.

Библиографический список

Используемые интернет-ресурсы:

1. https://mediascope.net/news/1250827/
2. http://www.licei347-540.ru/rod/internet_i_deti.php
3. https://promopult.ru/library/%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C
4. http://withsecurity.ru/kiberbezopasnost-voprosy-problemy-i-ugrozy-bezopasnosti

https://cyberleninka.ru/article/n/kiberbezopasnost-shkolnikov-v-internet-prostranstve-i-problemy-semeynogo-mediaobrazovaniya/viewer

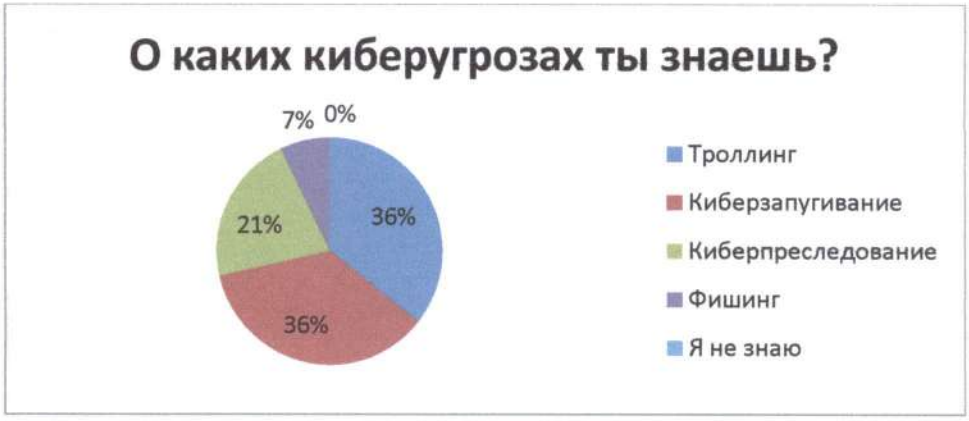
ПРИЛОЖЕНИЕ 1.

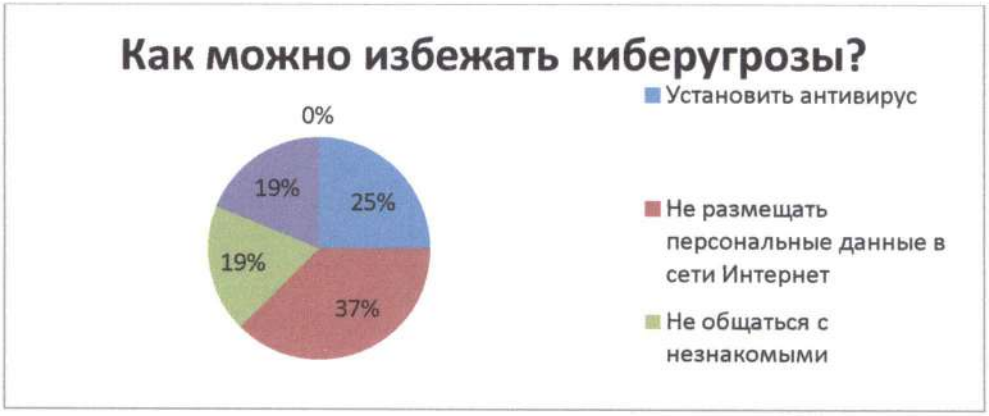
Алгоритм проверки информации на фейк.

Для проверки фейкового аккаунта в социальной сети анализируем следующие параметры:

- дата создания страницы;
- наличие/отсутствие личных фотографий владельца. Вместо них загружены картинки из сети или чужие снимки;
- дата загрузки изображений. Если снимки помещены пользователем на страницу в течение короткого промежутка времени, то это ложный профиль (снимки известных людей тоже являются признаком фальшивой страницы);
- количество записей на стене, их отсутствие или одна запись рекламного характера;
- лента изобилует приглашениями и игровыми постами от других пользователей.
- отсутствие снимков и информации о пользователе.

ПРИЛОЖЕНИЕ 2





ПРИЛОЖЕНИЕ 3.

Анкета для школьников

1.Сколько времени ты проводишь в Интернете?

2.Знаешь ли ты о киберугрозах?

А) да Б) нет

3.О каких киберугрозах ты знаешь?

А) троллинг

Б) киберзапугивание

В) киберпреследование

Г) фишинг

Д) я не знаю

4.Как можно избежать киберугрозы?

А) установить антивирус

Б) не размещать персональные данные в сети Интернет

В) не общаться с незнакомыми

Г) не скачивать неизвестные программы

Д) я не знаю как

ПРИЛОЖЕНИЕ 4.

Список интернет-ресурсов, занимающихся вопросами детской кибербезопасности:

1. **www.saferunet.ru** - Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете
2. **www.friendlyrunet.ru** - Фонд "Дружественный Рунет". Фонд поддерживает проекты, связанные с безопасным использованием интернета, содействует российским пользователям, общественным организациям, коммерческим компаниям и государственным ведомствам в противодействии обороту противоправного контента, а также в противодействии иным антиобщественным действиям в Сети
3. **www.fid.su/projects/saferinternet/year/hotline/** -
6. **http://www.ligainternet.ru/** - Лига безопасного Интернета
7. **http://i-deti.org/** - Портал "Безопасный инет для детей", ресурсы, рекомендации, комиксы

·8. **http://сетевичок.рф/** - "СЕТЕВИЧОК" сайт для детей — обучение и онлайн-консультирование по вопросам кибербезопасности сетевой безопасности

9. **http://www.igra-internet.ru/** — Онлайн интернет-игра "Изучи Интернет – управляй им"

http://www.safe-internet.ru/ — сайт Ростелеком "Безопасноть детей в Интернете", библиотека с материалами, памятками, рекомендациями по возрастам.

ПРИЛОЖЕНИЕ 5

Урок безопасности для учащихся начальной школы МБОУ СОШ п.Тумнин

Попросите ребёнка не провоцировать конфликтные ситуации и относится к другим так же, как он хотел бы, чтобы относились к нему самому.

Объясните, что ни при каких обстоятельствах не стоит размещать провокационный материал и не распространять по чьей - либо просьбе информационные и агрессивно - настроенные сообщения.

Информация, выложенная в Интернет - доступна всем и может быть использована в любых, в том числе мошеннических целях.

- Расскажите ребенку, что в Интернете встречаются и «хорошие» и «плохие» люди.
- Объясните, почему не стоит добавлять « в друзья» незнакомых людей - они могут быть не теми, за кого себя выдают.
- Предупредите ребенка, чтобы он ни в коем случае не соглашался на «живые» встречи с Интернет-незнакомцами.
- Посоветуйте ему общаться в Интернете с теми, с кем он лично знаком.
- Предостерегайте от скачивания платной информации, особенно через sms.
- Объясните, почему не стоит обращать внимания на яркие баннеры с сообщениями о выигрышах или призах.

И наконец, последний, но не менее важный совет - используйте технические возможности вашего компьютера и Оператора.

Для предотвращения нежелательного контента и вирусов необходимо установить антивирус, настроить антиспам фильтры в почте.

С помощью средств родительского контроля или соответствующих услуг Оператора можно создать «белый» список Интернет-сайтов, ограничить время пребывания ребенка в Интернет, настроить возрастной фильтр.

ПОМНИТЕ О НАШИХ СОВЕТАХ

И ТОГДА ИНТЕРНЕТ СТАНЕТ ВАШИМ НАДЕЖНЫМ И ПОЛЕЗНЫМ ДРУГОМ

Интернет – это безграничный мир информации. Здесь ты найдёшь много интересного и полезного для учёбы. В Интернете можно общаться со знакомыми и даже заводить друзей.

Но кроме хорошего, в виртуальном мире есть и плохое. Неправильное поведение в Интернете может принести вред не только тебе, но также твоим родным и близким.

Чтобы обезопасить себя в Интернете, достаточно соблюдать правила, которые содержатся в этой памятке. В этих правилах нет ничего трудного. Отнесись к ним внимательно – и расскажи о них своим друзьям!

Тест на знание правил поведения в Интернете

1) Новый друг, в чьих данных указан тот же возраст, что и у тебя, предлагает тебе обменяться фотографиями.

   A Попрошу его фото, и потом отправлю своё.
   B Посоветуюсь с родителями.

2) В чате тебя обозвали очень грубыми словами.

   A Скажу в ответ: «Сам дурак».
   B Прекращу разговор с этим человеком.

3) Знакомый предложил разослать телефон и адрес «плохой девочки», чтобы все знали о ней.

   A Потребую доказательств, что она плохая.
   B Сразу откажусь.

4) Пришло сообщение с заголовком «От провайдера» – запрашивают твой логин и пароль для входа в Интернет.

   A Вышлю только пароль: они сами должны знать логин.
   B Отмечу письмо как Спам.

Посчитай, сколько получилось ответов «А» и сколько «В».

4 «А»
Тебе ещё многому надо научиться.

3 «А» и 1 «В»
Внимательно прочитай эту памятку.

2 «А» и 2 «В»
Неплохо, но ты защищён лишь наполовину.

1 «А» и 3 «В»
Ты почти справился, но есть слабые места.

4 «В»
Молодец! К Интернету готов!

Министерство внутренних дел Российской Федерации

Управление «К»

Безопасный Интернет – детям!

Полезные советы для тебя и твоих друзей

ОСТОРОЖНО:

ВИРУСЫ И ДРУГИЕ ВРЕДОНОСНЫЕ ПРОГРАММЫ

В Интернет ты заходишь через компьютер. Это может быть школьный или библиотечный компьютер, твой личный или тот, которым пользуется вся семья.

Любому компьютеру могут повредить вирусы, их еще иногда называют вредоносными программами. Они могут **уничтожить** важную информацию **или украсть** деньги через Интернет.

- **Для защиты компьютера** на нём установлены специальные защитные программы и фильтры. Не меняй ничего в их настройках!
- **Не сохраняй подозрительные файлы** и не открывай их.
- Если антивирусная защита компьютера не рекомендует, **не заходи на сайт, который считается «подозрительным».**
- Никому **не сообщай свой логин с паролем** и не выкладывай их в Интернете – относись к ним так же бережно, как к ключам от квартиры.

ВИРТУАЛЬНЫЕ МОШЕННИКИ И ДРУГИЕ ПРЕСТУПНИКИ ИНТЕРНЕТА

Ты знаешь, что вне дома и школы есть вероятность столкнуться с людьми, которые могут причинить тебе вред или ограбить. В Интернете также есть злоумышленники – ты должен помнить об этом и вести себя так же осторожно, как и на улице или в незнакомых местах.

- **Не сообщай свой адрес или телефон** незнакомым людям и никогда не выкладывай в Интернете. Никогда **не высылай свои фотографии** без родительского разрешения. Помни, что **преступники могут использовать эту информацию** против тебя или твоих родных.
- **Если ты хочешь поучаствовать** в каком-нибудь конкурсе, где нужно указывать свои данные, посоветуйся с родителями.
- Никогда **не соглашайся прийти в гости к человеку, с которым ты познакомился в Интернете.** Если назначается встреча, она должна проходить в людном месте и желательно с присутствием родителей. Помни, что под маской твоего ровесника **может скрываться взрослый человек с преступными намерениями.**

ГРУБИЯНЫ И ХУЛИГАНЫ В ИНТЕРНЕТЕ: КАК СЕБЯ ВЕСТИ?

Кроме преступников в Интернете есть просто злые и невоспитанные люди. Ради собственного развлечения они могут обидеть тебя, прислать неприятную картинку или устроить травлю. Ты можешь столкнуться с такими людьми на самых разных сайтах, форумах и чатах.

- Помни: **ты не виноват**, если получил оскорбительное сообщение. Не нужно реагировать на грубых людей – просто прекрати общение.
- **Если тебе угрожают** по Интернету, не стесняйся сообщить об этом родителям. Помни, что цель угроз – испугать тебя и обидеть. Но **подобные люди боятся ответственности.**

- Коллективное преследование – это крайнее проявление жестокости. Жертву забрасывают оскорблениями и угрозами, его фотографию искажают и все данные публикуют. **Никогда не участвуй в травле и не общайся с людьми, которые обижают других.**
- Всегда **советуйся с родителями** во всех указанных случаях.