МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ

ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

"СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 31"

г.о. Мытищи Московская область.

Научно-исследовательская работа на тему:

«Использование цифровых технологий в современной жизни»

**Выполнил ученик 8 «Г» класса МБОУ СОШ №31**

Иванов Михаил

**Руководитель:** учителя информатики

Петренко Анна Николаевна

г. Мытищи

2019г

Мытищи, 2019

Доклад для VII региональной НПК

«Взгляд в науку» по теме:

Использование цифровых технологий в современной жизни

Выполнил: Иванов Михаил 8 «Г» класс

Место выполнения работы: Россия, г.Мытищи, Московская область, школа МБОУ СОШ №31

Научный руководитель: Петренко Анна Николаевна

Содержание

I. Введение......................................................................................................3

* II. Использование цифровых технологий в современной жизни....3
* Влияние цифровых технологий на повседневную жизнь................3
* Сбор информации – большие данные................................................6
  + Целевая реклама, основанная на личных данных...................6
  + Взлом личной информации.......................................................7
  + Защита от терроризма................................................................8
* Цензура в интернете.............................................................................8
* «Пузыри фильтров»..............................................................................10

III. Заключение................................................................................................12

Источники и литература.................................................................................13

**I. Введение**

**Цель** моего исследования – выяснить, как интернет может влиять на общество, а так же раскрыть состояние глобальной сети в целом на данный момент.

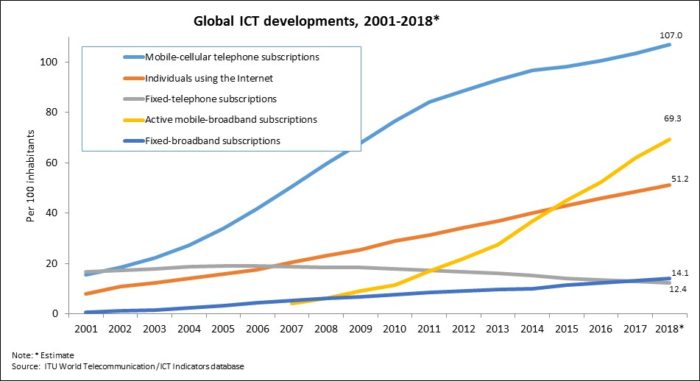
Я считаю, что моё **исследование актуально** для нахождения опасных тенденций в цифровую эру.

Для реализации поставленной цели решались следующие **задачи**:

* Изучение и анализирование литературы, посвящённой безопасности в интернете и большим данным.
* Рассмотрение статистики, связанной с темами.

**II. Использование цифровых технологий в современной жизни**

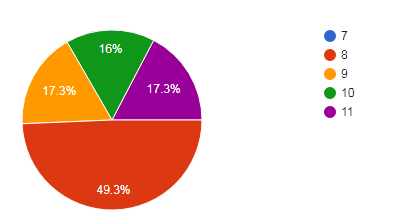
Интернет и беспроводные мобильные телефоны корённым образом переменили жизнь населения планеты. Даже в развивающихся странах, таких как Индия, в настоящее время скорость роста рынка мобильных технологий превышает скорость роста любого другого цифрового рынка.



**Влияние цифровых технологий на повседневную жизнь**

В связи со всё большей интеграцией информационных технологий (IT) в нашу жизнь, многие говорят о некой «наркотической зависимости» от этих технологий. Я считаю, что точно так же как человек 18 века не был наркотически зависим от водяных мельниц, человек современный не зависим от электронных устройств. Мобильный телефон может использоваться как планировщик, устройство связи, камера, калькулятор и многое другое. А при подключении к сети телефон может быть способом мгновенного общения, ресурсом любой информации, да и таким ещё количеством устройств, что перечислять их нецелесообразно. Телефоны и компьютеры изменили жизнь каждого человека к лучшему. Теперь информация не должна быть получена через СМИ или «сарафанное радио», а может быть получена и передана мгновенно.

Я провёл в своей школе исследование (опрос в гугл-формах) среди 7-11 классов, в котором участвовало 100 человек. В ходе опроса я выяснил, что:



Самые популярные в этих кругах соц. сети:

ВКонтакте: используется 92% процентами учащихся

WhatsApp: используется 84% процентами учащихся

Youtube: используется 62% процентами учащихся

Instagram: используется 74% процентами учащихся

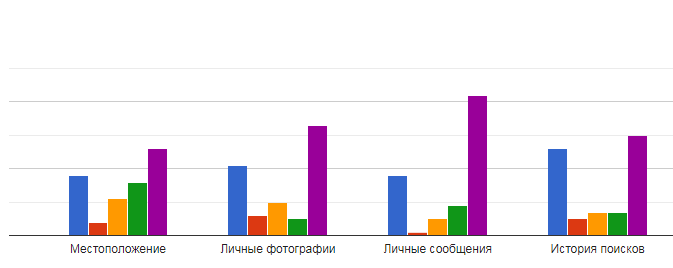
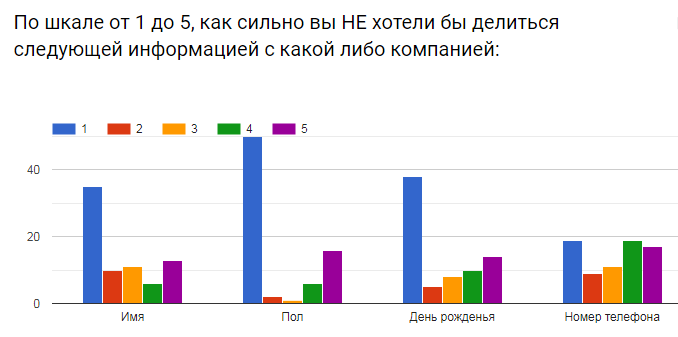


Здесь интересно подметить, что веря анализу портала Positive Technologies-

* Наиболее распространенными паролями у российских пользователей являются пароли, состоящие только из цифр, на долю которых приходится приблизительно 53% от числа всех проанализированных паролей;
* 88% используемых паролей – это пароли, содержащие в себе либо цифры, либо символы английского алфавита в нижнем регистре, либо и то и другое;
* Используемые пароли российскими пользователями в большинстве случаев не превышают 8-ми символов и лишь единицы используют пароли длиннее 12-ти символов;
* Удаленная атака по словарям позволяет скомпрометировать 37% учетных записей;
* 74% используемых паролей пользователями в корпоративном секторе не соответствуют требованиям стандарта PCI DSS;
* Администраторами информационных систем зачастую используются незамысловатые пароли низкой стойкости, которые могут содержаться в публично распространяемых словарях (15%), полностью совпадать с логином (10%) или вовсе отсутствовать (2%);

Кроме того, проведя личную беседу с некоторыми участниками опроса, я пришёл к выводу, что они не меняют свой пароль с какой-либо регулярностью.

Ниже результаты опроса о конфиденциальности информации, где оценка выше означает, что информация конфиденциальнее.



Интересно то, что не зависимо от опасений пользователей, все эти виды информации подвергаются сбору и обработке по умолчанию. В некоторых сервисах даже нет возможности отключения сбора данных.



Любопытно то, что 60% учеников делают покупки в интернете, при этом из них только 26% делают под присмотром взрослых.

В целом, российские школьники в интернете совсем не так хорошо защищены, как им кажется. Их данные могут быть легко доступны как обычным мошенникам, так и опытным специалистам по сбору информации.

*Человечество вступило в цифровую эру.*

**Сбор информации – большие данные**

Когда пользователь совершает любое действие на сайте или в приложении (оставляет комментарий под видео, открывает страницу, скачивает приложение, пишет сообщение и т.п.), вся информация копируется и хранится на серверах компаний, таких как Facebook, Google, Яндекс.

Таким образом, Facebook знает ваши политические взгляды, уровень доходов, религиозные взгляды и даже расу.

Вконтакте знает вашу историю изменения имени, все удалённые (даже для всех) сообщения, где вы живёте, когда и откуда вы заходили на сайт.

Google знает о всех ваших девайсах, он сохраняет все геолокации, где вы были, когда и что вы открывали на телефоне, имеет все записи вашего голоса за 2 секунды до и после фразы «Окей, google» и ещё больше, если вы используете приложения такие как «Google pay», «YouTube» и т.д.

В соответствии законом, принятым Европейским парламентом в январе 2018г., любой пользователь может запросить архив своих действий – всю информацию, которая есть о нём у компании.

*Так как используются эти данные?*

**Целевая реклама, основанная на личных данных**

Целевая реклама это реклама, которая основана на больших данных. Намного вероятнее, что пользователь купит продукт, если этот продукт рекомендуют ему, основываясь на его привычках и действиях. К примеру, если вы изменили свой статус отношений с «не женат» на «помолвлен», вы увидите больше рекламы ювилерии.

Однако в современном мире реклама иногда выходит за границы морали. Всё больше входит в тренд подготавливать покупателя к покупке через целевые новости и рекламу. Профессионалы в сфере рекламы способны манипулировать желаниями определённой целевой аудитории, пока эта аудитория не купит товар. Подобные стратегии могут быть использованы для рекрутизации, скажем, террористов.

Целевая аудитория террористических организаций – молодые люди, иммигранты, бедные люди, прошедшие через утрату любимых. Как раз для поиска таких людей идеально подходят стандартные инструменты целевой рекламы.

**Взлом личной информации**

Сейчас каждый школьник знает основные правила компьютерной безопасности - Не посещать подозрительные сайты и не открывать неизвестные программы. Однако способы получения личной информации с каждым месяцем становятся лучше, а если вас кто-то очень хочет взломать – они это сделают.

У крупных сайтов почти всегда работает эффективная защита от перебора, которую можно обойти, лишь имея очень крупную сеть ботов и растягивая атаку на многие месяцы, так что такой способ неэффективен.

Фишинг – заполучение пароля используя не настоящую ссылку на сайт, где пользователь «заходит» в свой аккаунт. Таким образом, с точки зрения пользователя ничего страшного не происходит: он вводит пароль и оказывается в своей привычной ленте друзей или в почтовом ящике.

Зловредное ПО оказывается на компьютере пользователя разными способами. Если злоумышленники не занимаются целевой атакой на конкретного человека, а стремятся заразить наибольшее число компьютеров (а это более распространённая тактика среди «традиционных» компьютерных преступников), то они предпочитают получить доступ к популярным сайтам и внедрить в них зловредный код. Посещение такого сайта с компьютера, где не установлены последние обновления безопасности, антивирус или браузер, который умеет предупреждать о заражённых сайтах, может привести к его заражению и попаданию под полный контроль атакующих.



Исследование показало, что люди готовы делиться данными с теми компаниями, которым доверяют. И наоборот, неуверенность в безопасности своих данных может стать причиной отказа от покупки у компании товаров (с этим согласились 88% опрошенных). Готовы прервать отношения с компанией, если та передаст личные данные третьим лицам без согласия пользователя, 73% россиян.

При этом большинство респондентов (35%) считают, что главная угроза для данных пользователей — это хакерские атаки. Почти все опрошенные отметили рост кибератак за последний год, только 3% считают, что число инцидентов сократилось.

В целом большинство респондентов — 85% — волнуют утечки данных и кибербезопасность. По их мнению, сегодня это один из самых значительных рисков для общества. Почти четверть опрошенных назвали растущий доступ к персональным данным одной из наиболее опасных угроз, с которыми в ближайшие десять лет придется столкнуться человечеству. Тем не менее 88% россиян согласны с тем, что полностью отключиться от интернета и перестать пользоваться мобильными устройствами сегодня уже невозможно.

**Защита от терроризма**

Страх стать жертвой террористической атаки испытывают

65% опрошенных. По сравнению с 2014 г. этот показатель

вырос на 7%. Число респондентов, считающих, что никакой

угрозы для территории РФ не существует, сократилось с

21% до 5%. Так как Россия находится на втором месте по числу погибших в терактах в 1994—2004 годах можно было бы сделать вывод, что терроризм – серьёзная угроза безопасности гражданина. Однако, я представляю информацию, выводы из которой напрашиваются сами. За 2016 год в России:

56 283 человек умерли от алкоголя, в том числе 14 021 именно отравились алкоголем! Это намного больше, чем в самых пьющих странах мира.

23 119 человек совершили самоубийство.

21 610 человек погибли на транспорте: 15 854 из них умерли в результате ДТП, 1700 были сбиты поездом.

4656 человек в России за год сгорели.

8537 человек в России умерли, просто неудачно упав на ровном месте.

В результате терактов за тот же год в России погибли 62 человека.

На предотвращение переговоров террористов в соц. сетях тратится намного больше денег, чем это требуется. Из-за этого процесса появляется больше способов взломать сеть, а так же сильно уменьшаются права на приватность пользователей.

Как программист могу заверить, что за пол часа можно наладить связь с математически непреодолимой шифровкой, так что никакие Телеграммы и Ватсаппы здесь не причём.

**Цензура в интернете**

Долгое время российский интернет не подвергался цензуре.

По данным организации Freedom House, в 2012 году интернет в России занимал 31 место из 60 стран по уровню свободы слова, и вошёл в категорию «частично свободный».

В 2012 году в силу вступил закон, позволяющий блокировать сайты с детской порнографией, пропагандой экстремизма, распространением наркотиков или призывами к самоубийству без решения суда. Параллельно также был введён закон, который предполагает привлекать уголовную ответственность на журналистов и интернет-пользователей, которые оскорбляют политических деятелей, вредят их имиджу и деловой репутации. Закон вызвал широкое негодование среди журналистов, утверждающих, что закон позволит подвергать российские СМИ жёсткой цензуре.

Введение законов о запрещённой информации и клевете, по данным Freedom House, опустило в 2013 году интернет в России с 31 места на 41 по уровню свободы слова. Уголовное преследование интернет-активистов возросло почти в 3 раза (103 случая против 38). Цензуре подвергается в основном политический, социальный или религиозный контент.

В октябре 2013 года был подготовлен проект приказа, который будет предоставлять ФСБ постоянный и прямой доступ к трафику передаваемому через интернет за период времени не менее чем 12 часов. Операторы заявили, что это нарушение конституции, права на неприкосновенность частной жизни. Приказ вступил в силу летом 2014 года.

В ноябре 2013 года Web Index составил рейтинг 81 стран по уровню свободы интернета, где Россия заняла 67 место. Сотрудники Google высказали своё опасения, что при настоящих тенденциях, в российском интернете в будущем может образоваться тотальная цензура, как в Китае.

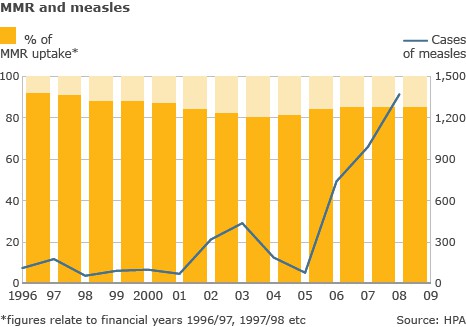
7 июля 2016 года был подписан «пакет Яровой», устанавливающий обязанность операторов связи по хранению всей передаваемой пользователями информации на срок до полугода.

26 января 2017 года было предложено ограничить доступ к интернету по «Китайской» аналогии.

**«Пузыри фильтров»**

Пузыри фильтров - негативная сторона персонализированного поиска, явления, при котором веб-сайты определяют, какую информацию пользователь хотел бы увидеть, основываясь на больших данных. В результате веб-сайты показывают только информацию, которая согласуется с прошлыми точками зрения данного пользователя. Вся иная информация, как правило, пользователю не выводится.

Так, если у пользователя есть два друга в социальной сети, один делает посты с поддержкой президента, а другой с его критикой, и пользователь делится первыми, а вторые игнорирует, то постепенно в его ленте будут появляться посты со всё более ярко выраженной высокой оценкой президента. Соответственно, он получает намного меньше противоречащей своей точке зрения информации и становится интеллектуально изолированными в своём собственном информационном пузыре.



Илай Парайзер в своей книге «The Filter Bubble» предупреждает, что проблемой фильтрации поисковых запросов является то, что она «закрывает нас от новых идей, предметов и важной информации» и «создаёт впечатление того, что наши узкие собственные интересы и есть всё, что существует и окружает нас». Это приносит потенциальный вред как для личности, так и для общества в целом.

В последние пять лет во всём мире были зафиксированы рекордные количества случаев смерти от Кори и Оспы.

19 января 2018 года всемирная организация здоровья назвала «движение против вакцинации» одной из самых больших мировых опасностей на данный момент.

Сейчас в социальных сетях таких как Facebook существует множество групп, в которых пропагандируются (конечно же неправильные) факты об опасностях вакцинации. Пользователи, которые ставят в таких группах лайки, нажимают на ссылки и т.д. попадают в пузырь фильтров, который не показывает им настоящую статистику о вакцинации и рекомендует всё больше пропаганды опасного движения.

В реальной жизни человек может использовать критическое мышление, чтобы строить свою точку зрения, но в современном интернете даже нейтральные мнения могут конфликтовать с другими нейтральными мнениями.

Яркий пример этого явления – Американская политическая система с двумя партиями. Люди в разных пузырях фильтров находят только утверждающие свою точку зрения факты, после чего вызывают конфликты в реальной жизни, которые никогда бы не существовали бы при традиционной системе средств массовой информации.

Изначально самым главным преимуществом глобальной сети было то, что в нём не было цензуры. Сейчас даже без вмешательства правительств или компаний, люди сами себя окружают звуконепроницаемыми стенами.

**III. Заключение**

В заключение можно подвести итог то, что

* Современные технологии зачастую страдают от вмешательства правительств и введения цензуры
* Компании, владеющие большими социальными сетями должны регулировать работу своих алгоритмов рекомендаций
* Новое поколение должно уметь лучше оценивать вес мнений, которые они видят в интернете.
* Большинство учащихся средней/старшей школы имеют множество знаний о работе с платёжными средствами.
* По результату опроса, более чем 3/4 учеников считают, что их пароль безопасен, в то время как по статистике это неправда.

Источники и литература:

<https://www.youtube.com/watch?v=_nVq7f26-Uo>

<https://www.youtube.com/watch?v=0-CiVZt6BrE>

https://www.youtube.com/watch?v=00AUE1ZBNKI

https://www.smartinsights.com/marketplace-analysis/customer-analysis/digital-marketing-statistics-sources/

<https://www.visualcapitalist.com/heres-what-the-big-tech-companies-know-about-you/>

<https://smallbusiness.chron.com/examples-targeted-advertising-10869.html>

<http://2017.russianinternetforum.ru/news/1298/>

[https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82\_%D0%B2\_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8#%D0%9F%D0%BE%D1%81%D0%B5%D1%89%D0%B0%D0%B5%D0%BC%D1%8B%D0%B5\_%D1%81%D0%B0%D0%B9%D1%82%D1%8B](#%D0%9F%D0%BE%D1%81%D0%B5%D1%89%D0%B0%D0%B5%D0%BC%D1%8B%D0%B5_%D1%81%D0%B0%D0%B9%D1%82%D1%8B)

<http://www.lookatme.ru/mag/how-to/security/206725-hacking-accounts>

<https://www.ranepa.ru/images/News/2017-02/20-02-2017-pres2.pdf>

<http://mgutm.ru/stopteror/inform_aktul.php>

<https://varlamov.ru/2894961.html>

https://ru.wikipedia.org/wiki/%D0%9F%D1%83%D0%B7%D1%8B%D1%80%D1%8C\_%D1%84%D0%B8%D0%BB%D1%8C%D1%82%D1%80%D0%BE%D0%B2

https://www.youtube.com/watch?v=B8ofWFx525s

https://www.rbc.ru/technology\_and\_media/25/05/2018/5b0700c19a794753dfab3be3

http://devteev.blogspot.com/2009/06/blog-post\_18.html