Муниципальное бюджетное общеобразовательное учреждение города Абакана
«Средняя образовательная школа №31»

Секция математика

Научно-исследовательская работа:

КРИПТОГРАФИЧЕСКИЕ И СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ.

Автор и исполнитель проекта: Бутова Алёна Вадимовна

ученица 8 класса «Б»

МБОУ СОШ № 31

Руководитель: Болсуновская Ольга Валерьевна

учитель математики

Абакан 2022

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Очень много снято фильмов, сюжетом которых является хранение, похищение, расшифровка секретной информации.

Как только люди научились писать, у них сразу же появилось желание сделать написанное понятным не всем, а только узкому кругу. Даже в самых древних памятниках письменности ученые находят признаки намеренного искажения текста, изменение знаков, нарушение порядка записи и т.д.

Понятие "Безопасность" охватывает широкий круг интересов, как отдельных лиц, так и целых государств. В наше настоящее время особое место отводится проблеме обеспечению защиты конфиденциальной информации.

Для этого существует множество методов. В моей работе мы рассмотрим простейшие криптографические и стенографические методы.

Актуальность: в связи с обострившимися отношениями между странами, важно сохранять тайну переписки и не допускать утечку информации.

Цель: изучить криптографические и стеганографические методы защиты информации.

Объект: защищаемая информация

Предмет: криптографические и стеганографические методы как способ защиты информации

Гипотеза: я предполагаю, что сообщение, зашифрованное криптографическим методом невозможно дешифровать без ключа,

Задачи:

1. Изучить литературу по проблеме исследования.
2. Раскрыть содержание понятий «защищаемая информация», «криптография», «стеганография», «шифрование», «дешифрование».
3. Рассмотреть способы шифрования и их математическое обоснование.
4. Рассмотреть основные стеганографические методы.
5. Осуществить шифровку и дешифровку текста.
6. Разработать собственный шифр.
7. Апробировать действие симпатических чернил.

1. ТЕОРЕТИЧЕСКОЕ ИССЛЕДОВАНИЕ

1.1. Понятие защищаемой информации

Информация, которая нуждается в защите, возникает в самых разных жизненных ситуациях. В таких случаях говорят, что она содержит тайну и является защищаемой, приватной, конфиденциальной, секретной.

Защищаемая информация – это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиям устанавливаемым собственником информации.

Для наиболее типичных, часто встречающихся ситуаций такого типа введены даже специальные понятия:

- государственная тайна;
- военная тайна;
- коммерческая тайна;
- юридическая тайна;
- врачебная тайна и т. д.

Защищаемая информация имеет следующие признаки:

- имеется определенный круг законных пользователей, которые имеют право владеть этой информацией;
- имеются незаконные пользователи, которые стремятся овладеть этой информацией с тем, чтобы обратить ее себе во благо, а законным пользователя во вред.

Задача криптографии и стеганографии, т.е. тайная передача, возникает только для информации, которая нуждается в защите. В таких случаях говорят, что информация содержит тайну или является защищаемой, приватной, конфиденциальной, секретной.

1.2. Криптографические методы защиты информации

Среди всего спектра методов защиты данных от нежелательного доступа особое место занимают криптографические методы. В отличие от других методов, они опираются лишь на свойства самой информации и не используют свойства ее материальных носителей, особенности ее передачи и хранения.

Криптография - наука о защите информации от прочтения ее посторонними.

Под криптографической защитой в первую очередь подразумевается шифрование данных.

Шифрование является преобразованием сообщения по определенным правилам, что делает его бессмысленным набором знаков для непосвященного в тайну шифра человека.

Абонент, получивший такой зашифрованный текст (получатель), с помощью обратного преобразования (расшифрования, расшифровки) восстанавливает исходный открытый текст.

Дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Было доказано, что в криптографии существуют только два основных типа преобразований - замены и перестановки, все остальные являются лишь комбинацией этих двух типов.

Криптография не «прячет» передаваемые сообщения, а преобразует их в форму, недоступную для понимания противником.

1.2.1. Шифр Цезаря

Этот шифр реализует следующее преобразование открытого текста: каждая буква открытого текста заменяется третьей после нее буквой в алфавите, который считается написанным по кругу, т.е. после буквы «а» следует буква «г». Поэтому класс шифров, к которым относится шифр Цезаря, называется шифрами замены.

Необходимо зашифровать слово **ПРИВЕТ**

Русский алфавит:

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Шифр: **ТУЛЕЗХ**

В шифрах типа шифра Цезаря ключом является величина сдвига букв шифр текста относительно букв открытого текста, в данном случае это цифра **3**.

1.2.2. Шифр Полибия

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	_	.	,

Полибий (I век до н. э.) – древнегреческий историк, государственный деятель и военачальник. С его именем связывают способ шифрования информации, суть которого заключается в следующем:

В квадрат размером 6 х 6 клеток построчно записываются буквы в алфавитном порядке, в последние три клетки заносятся такие знаки, как пробел, точка и запятая.

По типу «таблицы Пифагора» каждую букву кодируемого текста заменяют комбинацией номера строки и номера столбца, на пересечении которых она расположена.

Например, закодируем слово **АБАКАН,** в результате получим числовую комбинацию в виде шифра **«11 12 11 26 11 33».**

1.2.3. Магический квадрат 4х4.

В квадрат 4Х4 вписываются числа от 1 до 16. Его магия состоит в том, что сумма чисел по строкам, столбцам и полным диагоналям равняется одному и тому же числу — 34. Данный метод шифрования предназначен для небольшого объема информации (не более 16 символов).

16	**3**	**2**	**13**
5	**10**	**11**	**8**
9	**6**	**7**	**12**
4	**15**	**14**	**1**

Буквы фразы вписываются последовательно в квадрат согласно записанным в них числам: позиция буквы в предложении соответствует порядковому числу. В пустые клетки ставится точка или любая буква.

ОЧЕНЬ, СКОРО, ЛЕТО

16 о	**3е**	**2ч**	**13 л**
5 ь	**10 р**	**11о**	**8к**
9 о	**6 ,**	**7 с**	**12,**
4н	**15т**	**14е**	**1о**

После этого шифрованный текст записывается в строку (считывание производится слева-направо сверху-вниз, построчно) – **ОЕЧЛЬРОКО,С,НТЕО**

1.2.4. Кольцо

Разделив кольцо на 35 ровных частей, необходимо занумеровать их и пометить каждую буквой или знаком препинания. Затем выбирается какое-либо число *a* («ключевое число» шифра) и повернём кольцо вокруг центра по часовой стрелке так, чтобы каждая часть переместилась на *a* шагов. Например, если *a*=11, то часть, помеченная числом 01, перейдет в часть, помеченную числом 12, а это значит, что букве «А» при кодировании отвечает число 12. Точно так же букве «Б» отвечает число 13 и так деле.

Таким образом, каждая буква или знак записываются двузначным числом. Адресату для расшифровки надо разбить полученную последовательность цифр на двузначные числа, вычесть из каждого ключевое число и заменить полученное число буквой алфавита или знаком препинания.

Впрочем, на самом деле правила кодирования и раскодирования не так просты: ведь если *n* больше чем 24, то сумма *n*=11 больше чем 35, а у нас самое большое число равно 35. Но здесь надо вспомнить, что мы писали числа не на прямой, а на кольце, т.е. за числом 35 идет 1. Иными словами, после числа 35 все повторяется снова. Это значит, что, получив сумму, превосходящую 35, надо вычесть из неё 35. Полученная разность и покажет номер буквы.

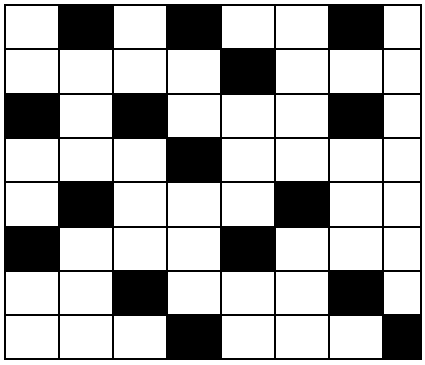
Например, буква «ы» переходит не в число 38, а в 03. Таким образом, при кодировании буква с номером n переходит в число *n*+11, если $1 \leqslant n \leqslant 24$, и в число n-24, если n>24. А при раскодировании число т переходит в букву с номером т-11, если $12 \leqslant т \leqslant 35$, и с номером т=24, если $1 \leqslant т \leqslant 11$.

1.2.5. Способ решетки

Наложив решетку на листок бумаги, пишут сообщение в окошечках решетки. Сначала помещается всего 16 букв. Затем поворачивают решетку на 90 градусов против часовой стрелки. Все написанные буквы закрыты, в новые окошечки продолжают вписывать текст. Еще два поворота и текст вписан. Если остаются неиспользованные клетки, их заполняют буквами а, б, в….и т.д. (чтобы не было пробелов).

На 64-клеточном поле можно составить более 4 млрд секретных решеток.

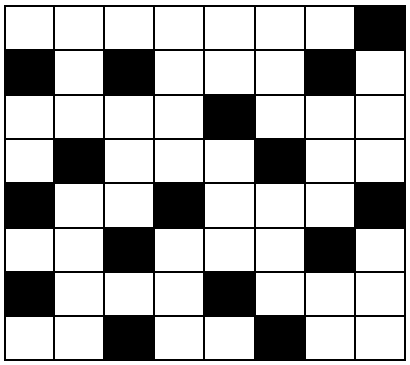
Шаблон решетки



Например, закодируем предложение «Родина - это место, где человек родился и вырос», в результате получим:

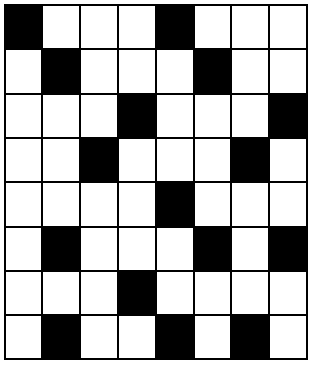
	Р		о			д	
				и			
н		а				э	
			т				
	о				м		
е				с			
		т				о	
			г				д

Перевернув решетку на 90 градусов мы получим:



	Р		о			д	е
ч		е		и		л	
н		а		о		э	
	в		т		е		
к	о		р		м		о
е		д		с		и	
л		т		с		о	
		я	г		и		д

Вновь перевернув решетку на 90 градусов мы получим:



в	Р		о	ы		д	е
ч	р	е		и	о	л	
н		а	с	о		э	
	в		т		е		
к	о		р		м		о
е		д		с		и	
л		т		с		о	
		я	г		и		д

В пропуски вписываем буквы в алфавитном порядке и в результате получаем:

в	Р	а	о	ы	б	д	е
ч	р	е	в	и	о	л	г
н	д	а	с	о	е	э	ё
ж	в	з	т	и	е	й	к
к	о	л	р	м	м	н	о
е	о	д	п	с	р	и	с
л	т	т	у	с	ф	о	х
ц	ч	я	г	ш	и	щ	д

1.2.6. Шифры и арифметика Остатков

Математика издавна применялась в теории шифров. Еще в конце XVI века расшифровкой переписки между противниками, Генриха III занимался один из создателей современной алгебры Франсуа Виет. А английские монархистские заговорщики в XVII веке поражались быстроте, с которой вождь английской революции Оливер Кромвель проникал в их замысел. Они думали, что используемые ими шифры невозможно разгадать, и считали, что ключи к ним выдал кто-то из участников заговора. В последствии выяснилось, что все эти шифры разгадывал один из лучших математиков того времени профессор Оксфордского университета Валлис. Он считал себя основателем новой науки-криптографии (тайнописи).

Разобьем все натуральные числа на классы, отнеся к одному классу числа, дающие одинаковые остатки при делении на 35.

Например, в один и тот же класс попадут числа 3, 38, 73, так как все они при делении на 35 дают в остатке 3. Общий вид чисел этого класса 3+35п, где п-нуль или натуральное число. Число различных классов равно 35(при делении на 35

получаются остатки 0, 1, 2, …, 34). Поэтому их можно обозначить теми же цифрами, что и соответствующие остатки, только писать сверху черточку. Например, $\bar{5}$ означает не число 5, а класс, содержащий это число (то есть число 5, 40, 75, …). В частности, $\bar{0}$ означает класс, содержащий число 35

Теперь уже можно написать, что $\bar{2}+11=\bar{3}$, то есть, прибавляя11 к числам класса $\bar{2}$, мы получаем числа из класса $\bar{3}$. Значит, если номерами кодируемых букв и знаками шифра считать классы, то кодирование и раскодирование сведутся к сложению и вычитанию классов.

Такая «арифметика остатков» полезна не только при шифровании. Пусть, например, сейчас минутная стрелка показывает 25 минут. Каким образом будет её положение через 176 минут? Чтобы ответить на этот вопрос, достаточно заметить, что через 60 минут стрелка возвращается в исходное положение. Поэтому надо найти остаток от деления суммы 25+176=201 на 60. Получим, что этот остаток равен 21. Значит, стрелка будет показывать 21 минуту.

Для облегчения сложения и вычитания в арифметике остатков при делении на p надо составить таблицу сложения. С этой целью берут обычную таблицу сложения и заменяют каждое число его остатком при делении на p (на рисунке p=5).

Если известно, что шифр получен прибавлением одного и того же числа к номерам букв, то его можно разгадать, угадав хотя бы значение одной буквы, а еще лучше - нескольких букв. Например, если известно, что в письме идет речь о Москве и в нем встречается сочетание «УХШСЙЗ», то легко догадаться, что при шифровании номер каждой буквы увеличивали на 7.

Более сложный шифр получается, если заменить сложение умножением. Будем, например, умножать номера всех букв на 2. Конечно, если произведение окажется больше 35, надо заменять его остатком от деления на 35. Например, буква «Ц» получит при шифровке номер13, так как номер буквы «Ц» равен 24, а при делении 24*2=48 на 35 получается остаток 13. Это преобразование запутаннее, чем сложнее. Можно опасаться, что разные буквы при кодировании перейдут в одну и ту же букву. Но к счастью, в данном случае этого не происходит. Доказательство этого утверждения основано на том, что произведение двух чисел делится на 2 лишь в том случае, когда один из множителей четен. А если бы мы попробовали умножать номера букв не на 2, а на 5 (делитель числа 35), то получилось бы плохо. Например, числам 1 и 8 соответствовали числа 5 и 40. Но остаток от деления 40 на 35 равен 5. И, получив тайнопись, по цифре 5 нельзя было бы узнать, что она означает: 1, 8, а может быть, 15 или 22? Все эти числа после умножения на 5 дают числа с одинаковым остатком при делении на 35. Коды можно получить также, заменяя умножение возведением в степень.

Зашифруем слово «Шифр»: Ш-26 ;И-10; Ф-22; Р-18.

- 26*2:35=1(ост.17)-П
- 10*2:35=0(ост.20)-Т
- 22*2:35=1(ост.9)-З
- 18*2:35=1(ост.1)-А
- «ПТЗА»

1.3. СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Стеганографией называется техника скрытой передачи или скрытого хранения информации. Целью стеганографии является сокрытие самого факта передачи сообщений. Для этого используются физические особенности носителей информации. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья, список покупок, письмо. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

Первая запись об использовании стеганографии встречается в трактате Геродота «История», относящегося к 440 году до н. э. В трактате были описаны два метода скрытия информации. Демарат отправил предупреждение о предстоящем нападении на Грецию, записав его на деревянную подложку восковой таблички до нанесения воска. Второй способ заключался в следующем: на обритую голову раба записывалось необходимое сообщение, а когда его волосы отрастали, он отправлялся к адресату, который вновь брил его голову и считывал доставленное сообщение

Существует несколько направлений стеганографии:

- Классическая стеганография.
- Компьютерная стеганография.
- Цифровая стеганография

1.3.1. Классическая стеганография

Одним из наиболее распространённых методов **классической стеганографии** является использование симпатических (невидимых) чернил. Текст, записанный такими чернилами, проявляется только при определённых условиях (нагрев, освещение, химический проявитель и т. д.). Владимир Ленин писал молоком на бумаге между строк. Строки, написанные молоком, становились видимыми при нагреве над пламенем свечи [].

В качестве симпатических чернил могут быть использованы самые различные вещества:

Чернила	Проявитель
Лимонная кислота (пищевая)	Метиловый оранжевый
Воск	$CaCO_3$ или зубной порошок
Яблочный сок	Нагрев
Молоко	Нагрев
Сок лука	Нагрев
Сок брюквы	Нагрев

Пирамидон (в спиртовом растворе)	Нагрев
Вяжущие средства для дезинфекции рта и глотки	Нагрев
Квасцы	Нагрев
Слюна	Очень слабый водный раствор чернил
Моча (свежая)	Нагрев
Фенолфталеин	Разбавленная щелочь
Стиральный порошок (с оптическим отбеливателем)	Свет лампы ультрафиолета
Крахмал	Йодная настойка
Аспирин	Соли железа

Также существует ряд альтернативных методов сокрытия информации:

- запись на боковой стороне колоды карт, расположенных в условленном порядке;
- запись внутри варёного яйца;
- узелки на нитках и т. д.

В настоящее время под **стеганографией** чаще всего понимают скрытие информации в текстовых, графических либо аудиофайлах путём использования специального программного обеспечения.

1.3.2. Компьютерная стеганография

Компьютерная стеганография — направление классической стеганографии, основанное на особенностях компьютерной платформы.

Например:

- Метод скрытия информации в неиспользуемых местах гибких дисков — при использовании этого метода информация записывается в неиспользуемые части диска, к примеру, на нулевую дорожку. Недостатки: маленькая производительность, передача небольших по объёму сообщений.
- Метод использования особых свойств полей форматов, которые не отображаются на экране — этот метод основан на специальных «невидимых» полях для получения сносок, указателей. К примеру, написание чёрным шрифтом на чёрном фоне. Недостатки: маленькая производительность, небольшой объём передаваемой информации.

1.3.3. Цифровая стеганография

Цифровая стеганография - направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Но, как правило, данные объекты являются мультимедиа-объектами (изображения, видео, аудио, текстуры 3D-объектов) и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов.

2. ПРАКТИЧЕСКОЕ ИССЛЕДОВАНИЕ

Каждый день тысячи людей, заходя в свой компьютер, обнаруживают, что их личная информация украдена. Хакеры ежеминутно взламывают социальные аккаунты , электронные почты для того ,чтобы рассылать спам, распространять вирус по сети, украсть деньги с электронных банковских счетов и т.д. Некого правила для борьбы с таким мошенничеством не существует , но можно усложнить процесс для злоумышленников ,применив методы защиты информации.

Изучив информацию об информационной безопасности, угрозах и методах защиты, я провела анонимное анкетирование, которое позволило мне сделать вывод о том, насколько осведомлены люди разной возрастной категории в вопросах по данной теме. (Приложение 1)

В анкетировании приняли участие 20 человек младше 17 лет .

Вопросы:

1. Выполняете ли Вы правила безопасной работы на компьютере?
2. Как Вы считаете, что является информационной безопасностью в современном мире?
3. Какой антивирусной программой Вы пользуетесь?
4. Сталкивались ли Вы когда - нибудь с компьютерными вирусами?
5. Какие аккаунты у Вас взламывали злоумышленники?
6. Установлена ли на вашем компьютере программа-фильтр, недопускающая Вас на вредоносные сайты?
7. Что Вы делаете, когда приходит предложение о добавлении в «друзья» от незнакомых людей?
8. Контролируют ли родители Вашу деятельность в сети интернет?

Заключение

Любой выбранный комплекс криптографических методов должен сочетать как удобство, гибкость и оперативность использования, так и надежную защиту от злоумышленников циркулирующей в ИС информации. Поэтому на настоящий момент наиболее оптимальны смешанные криптосиситемы, Объем знаний в этой области

Криптография не «прячет» передаваемые сообщения, а преобразует их в форму, недоступную для понимания противником.

Чрезвычайно велик и продолжает интенсивно увеличиваться. Кроме того, для полноценного освоения всех вопросов в шифровании требуется весьма солидная подготовка.

В будущем мы планируем продолжить исследование. Рассмотреть организационные и антивирусные методы защиты информации, а также защита с помощью паролей.

Список литературы

1. Бабаш, А. В. История криптографии. Часть I / А.В. Бабаш, Г.П. Шанкин. - М.: Гелиос АРВ, 2016. - [240 с.]
2. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. - М.: Гелиос АРВ, 2015. - [376 с.]
3. Бузов, Геннадий Алексеевич Защита информации ограниченного доступа от утечки по техническим каналам / Бузов Геннадий Алексеевич. - М.: Горячая линия - Телеком, 2016. - [186 с.]
4. Бунин О. Занимательное шифрование // Журнал «Мир ПК» 2003 №7.
5. Вельшенбах, М. Криптография на Си и С++ в действии. Учебное пособие / М. Вельшенбах. - М.: Триумф, 2014. - [462 с.]
6. Горев, А И; Симаков А А Обеспечение Информационной Безопасности / А Горев А И; Симаков А. - Москва: ИЛ, 2016. - [494 с.]
7. Грибунин, Вадим Геннадьевич Цифровая стеганография / Грибунин Вадим Геннадьевич. - М.: Солон-Пресс, 2016. - [589 с.]
8. Григорович, А.В. Юный химик. Интересные опыты по химии. –Х., 2009. - [64 с.]
9. Жданов, О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования / О.Н. Жданов. - М.: ИНФРА-М, 2015. - [869 с.
10. Зубов, А.Н. Математика кодов аутентификации / А.Н. Зубов. - М.: Гелиос АРВ, 2014. - [319 с.]
11. Крысин А.В. Информационная безопасность. Практическое руководство -- М.: СПАРРК, К. ВЕК+,2003.
12. Кузьмин, Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. - Москва: Огни, 2013. - [192 с.]
13. Литвинская, О. С. Основы теории передачи информации. Учебное пособие / О.С. Литвинская, Н.И. Чернышев. - М.: КноРус, 2015. -[168 с.]
14. Лукашов И. В. Криптография? Железно! //Журнал «Мир ПК». 2003. № 3.
15. Осмоловский, С. А. Стохастическая информатика. Инновации в информационных системах / С.А. Осмоловский. - М.: Горячая линия - Телеком, 2012. - [322 с.]
16. Панасенко С.П., Защита информации в компьютерных сетях // Журнал «Мир ПК» 2002 № 2.
17. Панасенко С. П. Чтобы понять язык криптографов // Журнал «Мир ПК». 2002. № 6.
18. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования -- М.: ФОРУМ: ИНФРА-М, 2004.
19. Стохастические методы и средства защиты информации в компьютерных системах и сетях: моногр. / Под редакцией И.Ю. Жукова. - М.: КУДИЦ-Пресс, 2016. - [512 с.]
20. Хоффман, Л. Дж. Современные методы защиты информации / Л.Дж. Хоффман. - Москва: СПб. [и др.]: Питер, 2014. - [264 с.]

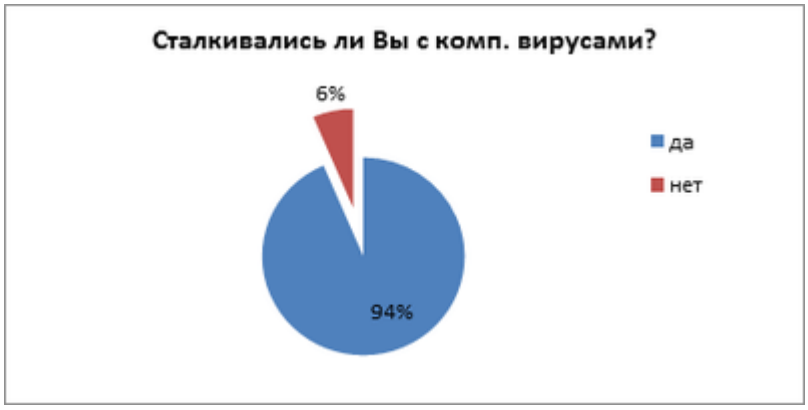
Приложение 1

Результаты анкетирования

Результаты ответов на 1 первый вопрос анкеты показывают, что учащиеся и взрослые хорошо осведомлены о правилах безопасной работы на компьютере. Однако, стоит отметить, что 20% респондентов искренне ответили, что правила безопасности они соблюдают очень редко, так как забывают о них, 11% не знают и не соблюдают правила.

Анализируя данные диаграммы по второму вопросу, можно сказать, что большинство опрошенных считают пароли основой информационной безопасности.

Следующий вопрос анкетирования выявил, что 16% респондентов не пользуются антивирусными программами. Считаю, что данная цифра является высокой, так как в современном мире без защиты данных от вирусов не обойтись. Самыми популярными программами оказались Антивирус Касперского (26%) и Dr.Web (22%).



Из диаграммы видно, что большинство респондентов (94%) сталкивались с вирусами на своих устройствах. На мой взгляд, это еще раз подтверждает необходимость использования антивирусных программ

Из диаграммы видно, что у большинства опрошенных аккаунты взламывались, но тем не менее 26% не подвергались «*взламыванию*», это говорит о том, что они серьезно относятся к работе в сети Интернет и надежно защищают свои данные.

Следующий вопрос анкеты, об установленной на компьютере программе – фильтре для детей поставил в тупик многих участников опроса.

Исследование показало, что у 91% респондентов не установлено таких программ на ПК, а это значит, что любой подросток может зайти в интернете на любой сайт с любым содержательным контентом и вредоносностью.

Также все порошенные подтвердили, что в социальных сетях выставляют информацию о своей семье (указывают родственников), в открытом доступе

представлена информация о школе, месте жительства, иногда номер телефона. И все 46 респондентов ответили положительно на вопрос о выставлении в социальных сетях своих настоящих Фамилии и имени, а также о выставлении личных фотографий.