Научно-исследовательская работа

Предмет: «Математика»

ЗАГАДОЧНЫЙ МИР ШИФРОВ

Выполнила:

Никулина Арина Дмитриевна

учащаяся 8 класса

МБОУ г. Астрахани «СОШ № 36», Россия, г. Астрахань

Руководитель:

Жак Альфия Мавлюдовна

Учитель математики

МБОУ г. Астрахани «СОШ № 36», Россия, г. Астрахань

Введение

Наверняка, каждый из нас в детстве играл в тайные записочки, содержание которых понимали только избранные. Это очень увлекательное занятие! Процесс преобразования исходного текста в текст, понятный только адресату, называют **шифрованием**, а способ такого преобразования – **шифром**.

Я не редко слышу, как люди говорят: «У меня нет никаких тайн, мне нечего скрывать!». Хотя за этой фразой наверняка прячется совсем другой смысл, многие считают, что просто никто не полезет к ним в телефон или компьютер в поисках чего-нибудь ценного. А ведь на практике часто происходит всё по-другому. Стоит оставить незакрытый файл на компьютере или разблокированный телефон с входящим сообщением, как сразу у безобидно проходящей мимо мамы или сестры возникнет желание заглянуть туда. Стоит задать себе вопрос все ли фотографии или переписки в вашем телефоне вы готовы показать своим домочадцам? Готовы отдать знакомым или близким пароли от банковской карты или социальных сетей? Я думаю, ответ очевиден!

Актуальность исследования. Проблема защиты информации от прочтения посторонним лицом всегда волновала человечество и актуальна до сих пор. Высокая значимость этой проблемы определяет новизну данного исследования.

Цель исследования. Изучение основных методов шифрования и использование их в повседневной жизни.

Основная часть

1. Поиск и анализ проблемы

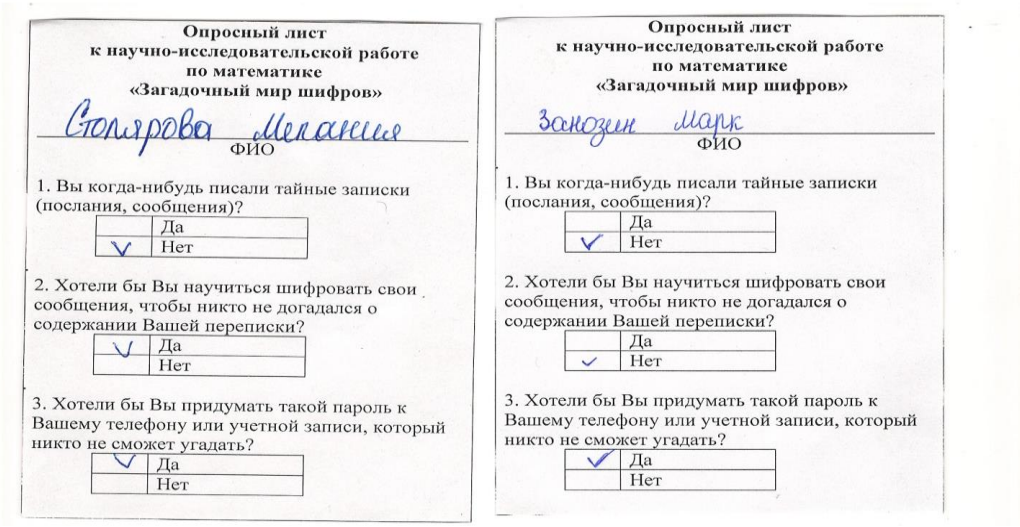
Для начала я решила провести анкетирование среди одноклассников. Я предложила им следующие вопросы.

1.Вы когда-нибудь писали тайные записки (послания, сообщения)?

В результате исследования мнения опрошенных учеников разделились почти поровну:

2. Хотели бы Вы научиться шифровать свои сообщения, чтобы никто не догадался о содержании Вашей переписки?

3. Хотели бы Вы придумать такой пароль к Вашему телефону или учетной записи, который никто не сможет угадать?



Опросный лист
к научно-исследовательской работе
по математике
«Загадочный мир шифров»

Солярова Милана
ФИО

1. Вы когда-нибудь писали тайные записки (послания, сообщения)?

	Да
V	Нет

2. Хотели бы Вы научиться шифровать свои сообщения, чтобы никто не догадался о содержании Вашей переписки?

V	Да
	Нет

3. Хотели бы Вы придумать такой пароль к Вашему телефону или учетной записи, который никто не сможет угадать?

V	Да
	Нет

Опросный лист
к научно-исследовательской работе
по математике
«Загадочный мир шифров»

Заюзин Марк
ФИО

1. Вы когда-нибудь писали тайные записки (послания, сообщения)?

	Да
✓	Нет

2. Хотели бы Вы научиться шифровать свои сообщения, чтобы никто не догадался о содержании Вашей переписки?

	Да
✓	Нет

3. Хотели бы Вы придумать такой пароль к Вашему телефону или учетной записи, который никто не сможет угадать?

✓	Да
	Нет

Рис. 1. Образец опросного листа

Исходя из ответов моих одноклассников, можно сделать вывод, что результаты моего исследования будут полезны и интересны. Подавляющее большинство людей, хотело бы придумать себе безопасный от взлома пароль. А в этом вопросе очень пригодятся знания шифрования.

2. Основные виды шифров

Практической значимостью данной работы является привлечение внимания к изучению проблем защиты информации. Для достижения поставленной цели, я разработала сборник основных известных видов

шифрования, дополнив его своими разработанными шифрами Данный сборник ориентирован как на средний школьный возраст, так и на людей старше.

Рис. 2. Сборник основных известных видов шифрования

2.1.Шифр Цезаря

Также известный как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования. В данном шифре каждая буква в слове заменяется другой, которая находится на определенном расстоянии левее или правее от неё в алфавите.

2.2.Шифр «Сциталь»

Скита́ла или сцитала— инструмент, используемый для осуществления перестановочного шифрования, в криптографии известный также как шифр Древней Спарты. Представляет собой цилиндр и узкую полоску пергамента, на которой писалось сообщение, обматывавшуюся вокруг него по спирали.

Рис. 3. Сборник основных известных видов шифрования

2.3.Шифр «Поворотная решетка» или «Решетка Кардано»

Разработать решетку не сложно. Главное, чтобы при развороте ячейки решетки не накладывались друг на друга. Каждая из клеток при поворотах переходит в строго определенные клетки. Не сложно заметить алгоритм перемещения. Но чтобы этот алгоритм работал количество клеток по горизонтали и вертикали должно быть четное. Рассмотрим на примере квадрата 6х6.Каждую из сторон делим на 2 (6:2=3), соответственно далее разбиваем квадрат 6х6 на 4 квадрата 3х3 и в 1 квадрате вписываем по порядку числа от 1 до 9 слева направо. Затем мысленно переворачиваем квадрат по часовой стрелке на 90 градусов и снова вписываем цифры:

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

В итоге вырезать клетки нужно таким образом, чтобы для каждого номера была вырезана ровно одна клетка. Выберем такой вариант:

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

Рис. 4. Создание «Решетки Кардано»

Попробуем зашифровать название работы, фамилию и имя автора «Загадочный мир шифров Никулина Арина» таким образом:

З	2	3	7	**А**	1
4	Г	6	8	5	2
7	А	9	9	Д	3
3	6	О	9	8	Ч
Н	5	8	6	5	4
1	4	7	Ы	2	1

Разворачиваем решетку на 90 градусов и продолжаем вписывать текст в пустые ячейки.

З	2	3	Й	**А**	1
М	Г	И	8	5	2
7	А	9	9	Д	Р
3	6	О	Ш	8	Ч
Н	И	Ф	6	5	4
Р	4	7	Ы	О	1

Рис. 5. Шифрование с помощью «Решетки Кардано»

Повторяем то же самое:

З	2	В	Й	**А**	1
М	Г	И	8	5	Н
И	А	9	К	Д	Р
З	У	О	Ш	Л	Ч
Н	И	Ф	6	И	4
Р	Н	7	Ы	О	А

Затем ещё один разворот по часовой стрелке. У нас останутся четыре пустые ячейки, в которые мы вписываем любые буквы.

З	А	В	Й	А	А
М	Г	И	Р	И	Н
О	А	Н	И	Д	Р
А	К	О	Ш	У	Ч
Н	Ш	И	Г	Л	А
Ф	И	Р	Ы	О	Н

Рис. 6. Шифрование с помощью «Решетки Кардано»

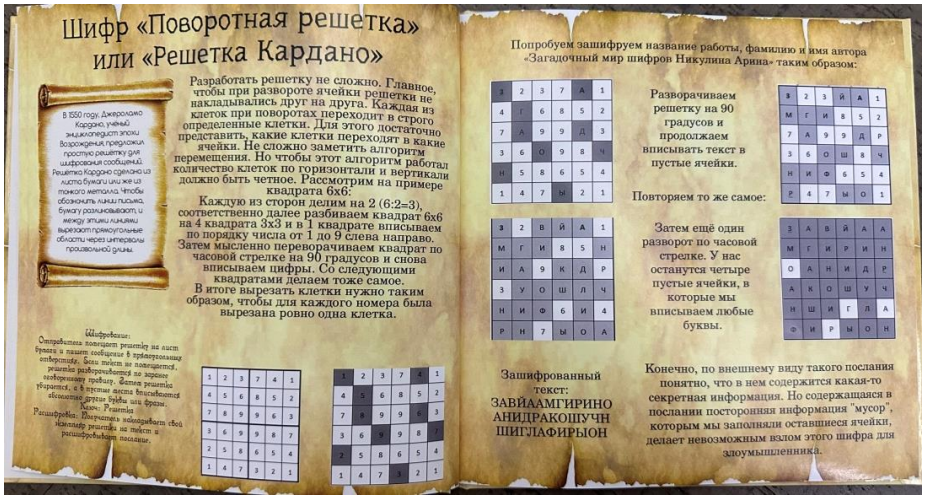


Рис. 7. Сборник основных известных видов шифрования

2.4.Транспозиция

В транспозирующих шифрах буквы переставляются по заранее определенному правилу. Например, если каждое слово пишется задом наперед, то из «загадочный мир шифров» получается «йынчодагаз рим ворфиш».

2.5.Маршрутная перестановка

Исходный текст вписывается в геометрическую фигуру по ходу одного «маршрута», а затем по ходу другого выписывается с нее.

2.6.Цифровые шифры

Алфавит разбивается на группы букв, затем каждой группе присваивается свой номер (знаменатель числа). Числитель – это порядковый номер буквы в группе. Каждая буква будет изображаться дробью.

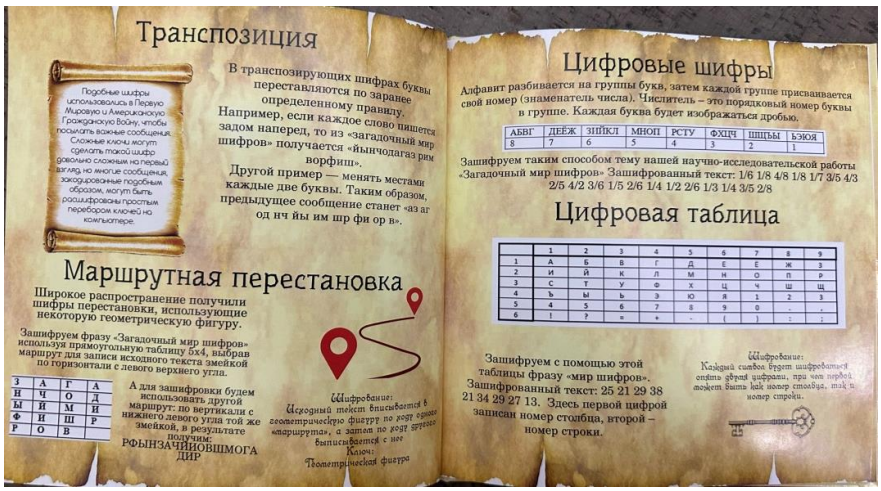


Рис. 8. Сборник основных известных видов шифрования

2.7. Шифр Виженера

Данный шифр является более сложным. Шифр Виженера использует следующий принцип: каждая буква меняется в соответствии с кодовым словом. Допустим, ключевое слово НАУКА. Тогда первая буква послания будет зашифрована согласно шифровальному алфавиту для первой буквы кодового слова (в нашем случае «Н»), вторая буква — согласно алфавиту для второй буквы кодового слова («А»), и так далее. В случае, если послание длиннее кодового слова, то для (k*n+1)-ой буквы (где n — это длина кодового слова) вновь будет использован алфавит для первой буквы кодового слова.

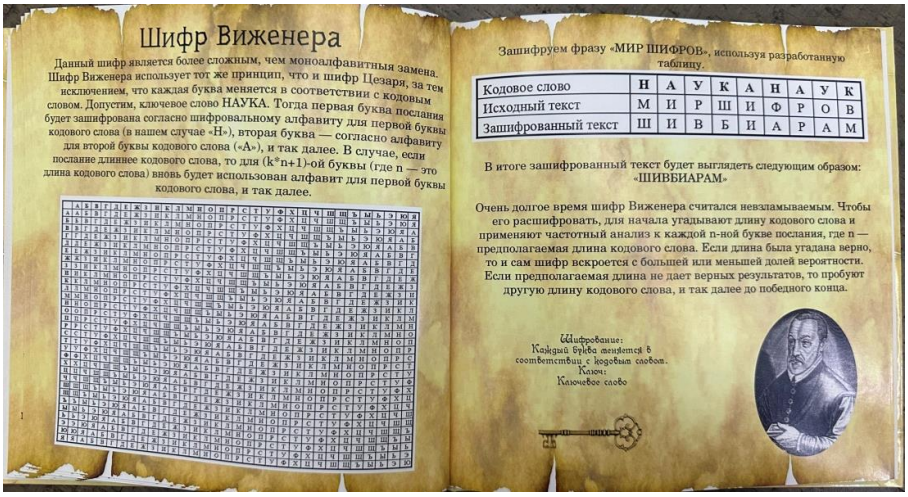


Рис. 9. Сборник основных известных видов шифрования

2.8. Шифр из «Пляшущих человечков»

Многие знакомы с этим шифр из рассказа Артура Конана Дойля. Каждая буква изображается каким-то своим знаком (рисунком).

2.9. Азбука Морзе (Код Морзе)

Назван в честь Сэмюэля Морзе. В этом шифре каждый символ (буквы алфавита, цифры от 0 до 9 и некоторые символы пунктуации) заменяется последовательностью коротких и длинных звуковых сигналов. Короткий сигнал на бумаге записывается как точка, длинный сигнал как тире.

Рис. 10. Сборник основных известных видов шифрования

2.10. Шифр «Линейка Энея»

В криптографии линейка Энея представляла собой устройство, имеющее определенные отверстия, количество которых равнялось количеству букв алфавита. К линейке была прикреплена катушка с намотанной на неё ниткой. Нить протягивалась через прорезь, а затем через отверстие, соответствующее первой букве шифруемого текста, при этом на нити завязывался узелок в месте прохождения её через отверстие; затем нить возвращалась в прорезь и аналогично зашифровывалась вторая буква текста и т. д. После окончания шифрования нить извлекалась и передавалась получателю сообщения.

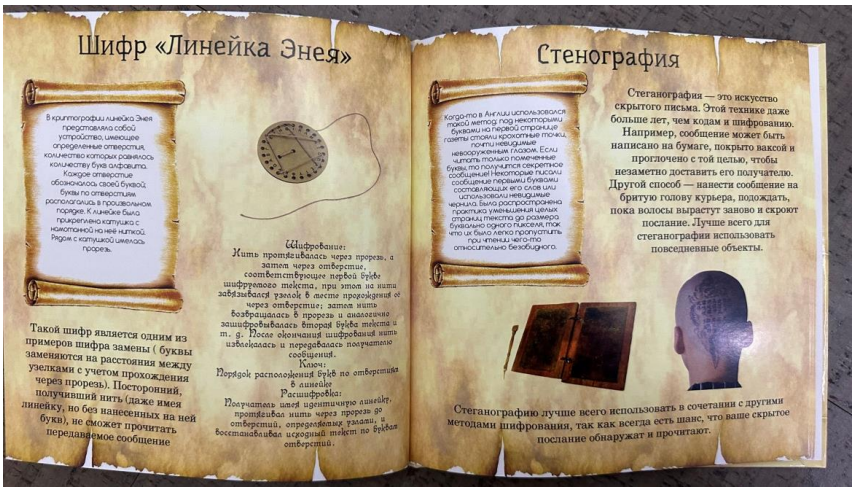


Рис. 11. Сборник основных известных видов шифрования

2.11. Шифр Гронсфельда

Шифр Гронфельда — шифр замены, использующий число в качестве ключа для текста. Для шифрования используется числовой ключ. Но каждая буква смещается не на постоянное число позиций, а на то число, которое соответствует определенному ключу. А ключ состоит из группы цифр. Если ключ короче сообщения, то его повторяют по циклу.

2.12.Порядковый номер

Шифрование с заменой каждой буквы ее номером в алфавите. Очень простой вид шифра. Но между тем, он часто применяется в различных вариациях и комбинациях с другими видами шифров. Вариация этого шифра: буквы в алфавите отсчитываются не с начала, а с конца. То есть порядковым номер буквы «А» будет 33, «Б» – 32 и так далее.

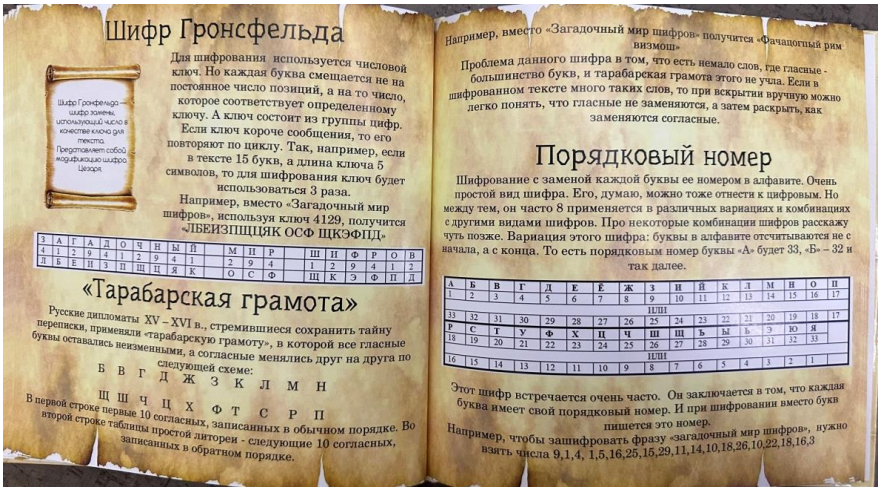


Рис. 11. Сборник основных известных видов шифрования

2.13.Книжный шифр

Книжный шифр, является еще одним примером шифра перестановки. Часто данный вид шифра можно встретить в детективах, когда у отправителя и получатель есть одинаковый томик какого-нибудь романа. Суть этого шифра состоит в том, что каждая буква в сообщении определяется тремя цифрами: первая - номер страницы, вторая –номер строки сверху или снизу в зависимости от договоренности, а третья – номер буквы в строке.

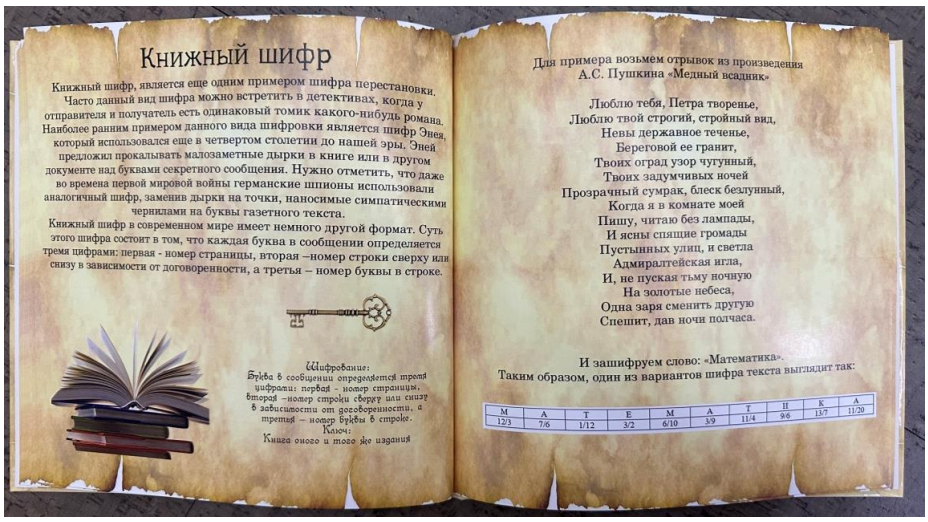


Рис. 12. Сборник основных известных видов шифрования

2.14.Шифр «Прямоугольная система координат»

Изучая данную тему, я решила разработать свой шифр «Прямоугольная система координат», используя знания математики.

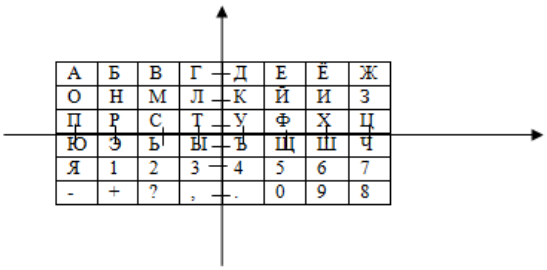


Рис. 13. Шифр «Прямоугольная система координат»

На прямоугольной системе координат я расположила алфавит, цифры и основные знаки. Для шифрования достаточно записать координаты необходимой буквы.

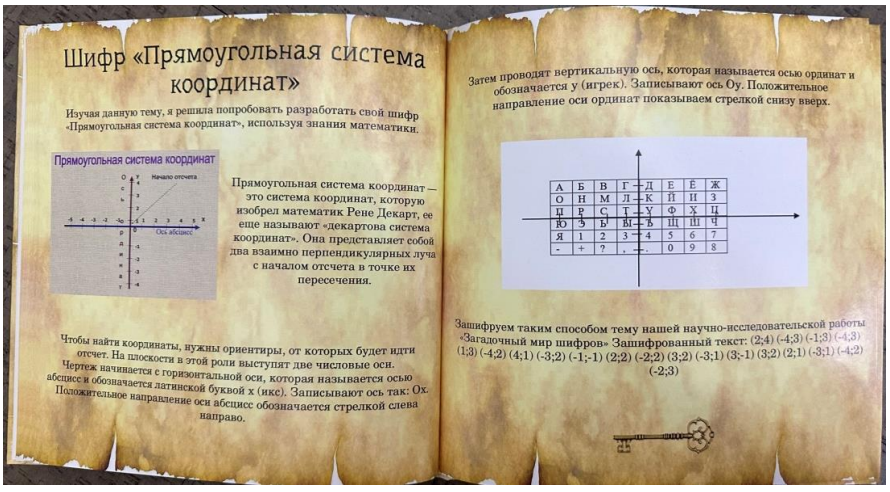


Рис. 14. Сборник основных известных видов шифрования

2.3. Алгоритм создания надежного пароля

В современном мире в телефоне хранится буквально вся наша жизнь. И никто не застрахован от того, чтобы случайно забыть телефон в кафе, на работе, в школе или еще где-нибудь. Где гарантия того, что другие люди не воспользуются вашим устройством в плохих целях? Какой выход? Создайте надежный пароль! Это **решит следующие проблемы**:

- защитит личные данные;
- сохранит конфиденциальность писем, файлов и других материалов;
- предотвратит несанкционированный доступ к аккаунту.

Какой пароль выбрать? Да, да, тот самый ненавистный с заглавными и строчными буквами, с цифрами и символами. И желательно, чтобы он был длинным. Но помните, пароль придется вводить достаточно часто, поэтому не придумывайте тех комбинаций, которые вы потом не вспомните.

Рис. 15. Буклет «Алгоритм создания надежного пароля»

Многие считают, что лучше воспользоваться мастером создания паролей или использовать надежный пароль, который предлагает создать ваш телефон.

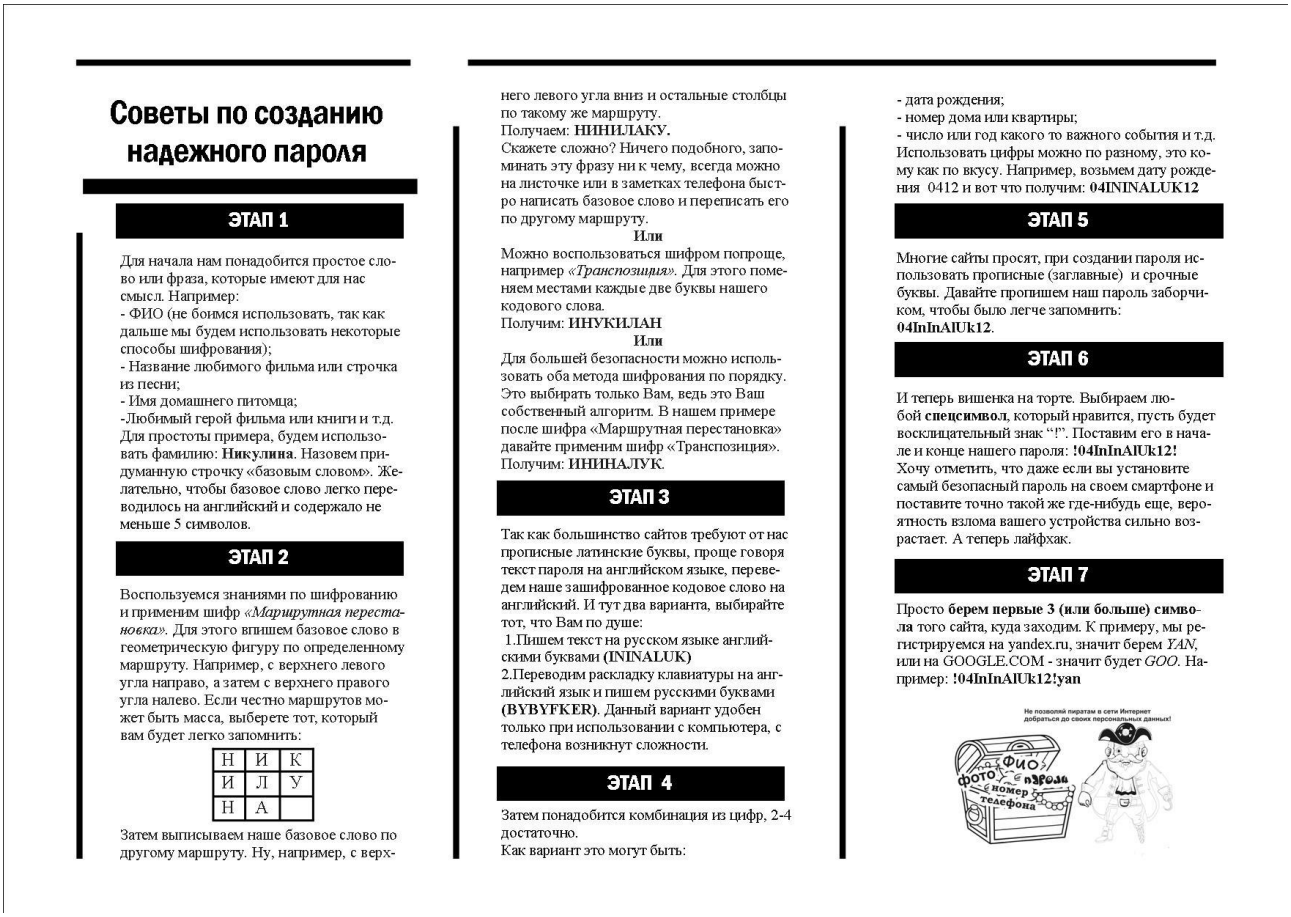
Но для меня это не лучший вариант, так как нередко бывают случаи, когда нужно зайти в учетную запись с другого устройства, а ваш надежный пароль хранится на телефоне, и его уж точно запомнить не получится. Поэтому я рекомендую установить такой пароль, чтобы вам было легко его запомнить, но посторонние не могли его угадать.

Как запомнить такой длинный пароль? Варианта два:

1.Заучить, как сложную формулу по физике.

2.Придумать пароль, основываясь на своей логике.

Думаю, второй вариант нам подходит больше.



Советы по созданию надежного пароля

ЭТАП 1

Для начала нам понадобится простое слово или фраза, которые имеют для нас смысл. Например:
- ФИО (не боимся использовать, так как дальше мы будем использовать некоторые способы шифрования);
- Название любимого фильма или строчка из песни;
- Имя домашнего питомца;
-Любимый герой фильма или книги и т.д.

Для простоты примера, будем использовать фамилию: **Никулина**. Назовем придуманную строчку «базовым словом». Желательно, чтобы базовое слово легко переводилось на английский и содержало не меньше 5 символов.

ЭТАП 2

Воспользуемся знаниями по шифрованию и применим шифр *«Маршрутная перестановка»*. Для этого впишем базовое слово в геометрическую фигуру по определенному маршруту. Например, с верхнего левого угла направо, а затем с верхнего правого угла налево. Если честно маршрутов может быть масса, выберете тот, который вам будет легко запомнить:

Н	И	К
И	Л	У
Н	А	

Затем выписываем наше базовое слово по другому маршруту. Ну, например, с верхнего левого угла вниз и остальные столбцы по такому же маршруту.

Получаем: **НИНИЛАКУ.**

Скажете сложно? Ничего подобного, запоминать эту фразу ни к чему, всегда можно на листочке или в заметках телефона быстро написать базовое слово и переписать его по другому маршруту.

Или

Можно воспользоваться шифром попроще, например *«Транспозиция»*. Для этого поменяем местами каждые две буквы нашего кодового слова.

Получим: **ИНУКИЛАН**

Или

Для большей безопасности можно использовать оба метода шифрования по порядку. Это выбирать только Вам, ведь это Ваш собственный алгоритм. В нашем примере после шифра «Маршрутная перестановка» давайте применим шифр «Транспозиция».

Получим: **ИНИНАЛУК**.

ЭТАП 3

Так как большинство сайтов требуют от нас прописные латинские буквы, проще говоря текст пароля на английском языке, переведем наше зашифрованное кодовое слово на английский. И тут два варианта, выбирайте тот, что Вам по душе:

1.Пишем текст на русском языке английскими буквами **(ININALUK)**

2.Переводим раскладку клавиатуры на английский язык и пишем русскими буквами **(BYBYFKER)**. Данный вариант удобен только при использовании с компьютера, с телефона возникнут сложности.

ЭТАП 4

Затем понадобится комбинация из цифр, 2-4 достаточно.

Как вариант это могут быть:
- дата рождения;
- номер дома или квартиры;
- число или год какого то важного события и т.д.

Использовать цифры можно по разному, это кому как по вкусу. Например, возьмем дату рождения 0412 и вот что получим: **04ININALUK12**

ЭТАП 5

Многие сайты просят, при создании пароля использовать прописные (заглавные) и срочные буквы. Давайте пропишем наш пароль заборчиком, чтобы было легче запомнить: **04InInAlUk12**.

ЭТАП 6

И теперь вишенка на торте. Выбираем любой **спецсимвол**, который нравится, пусть будет восклицательный знак "!". Поставим его в начале и конце нашего пароля: **!04InInAlUk12!**

Хочу отметить, что даже если вы установите самый безопасный пароль на своем смартфоне и поставите точно такой же где-нибудь еще, вероятность взлома вашего устройства сильно возрастает. А теперь лайфхак.

ЭТАП 7

Просто **берем первые 3 (или больше) символа** того сайта, куда заходим. К примеру, мы регистрируемся на yandex.ru, значит берем *YAN*, или на GOOGLE.COM - значит будет *GOO*. Например: **!04InInAlUk12!yan**

Рис. 16. Буклет «Алгоритм создания надежного пароля» (советы по созданию надежного пароля)

2.4. Создание пароля для блокировки телефона

Часто возникает вопрос: Какой 6-значный пароль придумать для блокировки/разблокировки телефона? Придумать пароль, состоящий из шести цифр - дело не трудное. Трудным будет вспомнить этот пароль, если по каким-

то причинам вы его забудете. Как известно, проще запомнить что-то осмысленное, а не бездушную последовательность цифр.

Я предлагаю воспользоваться знаниями по шифрованию и применить их при создании такого пароля. Так как задача стоит придумать именно пароль, состоящий из цифр, значит, и шифры нам подойдут именно цифровые. За основу возьмем шифр «Порядковый номер». Как мы знаем, при шифровании вместо буквы пишется её порядковый номер в алфавите. Для начала нам нужно выбрать кодовое слово (любое значимое для Вас). Для примера давайте возьмем имя: Арина. Затем проведем шифровку данным методом.

Таблица 1

Шифрования кодового слова

А	**Р**	**И**	**Н**	**А**
1	18	10	15	1

У нас получился цифровой код: 11810151. Но он для нас очень длинный, поэтому будем его сокращать.

Таблица 2

Этапы сокращения

Этап	**Порядок действия**	**Результат**
Исходный код: 11810151		
Существует правило, что в пароле не должно быть повторяющихся цифр (1111,2666,3030).		
1	В самом начале нашего кода есть два числа «1», предлагаю сократить одно из них.	1810151
Существует правило, что нужно избегать цифры 1 в начале пароля и цифры 0 на конце (именно с них обычно начинают подбор)		
2	Наш пароль как раз начинается с цифры 1, поэтому предлагаю ее убрать.	810151
Итоговый код: 810151		

Наш пароль получился не очень сложным, но легко запоминающимся. Но главное, комбинация получилась максимально отдаленной от цифр, связанных со мной. Это особенно важно, если эти цифры есть в общем доступе. Если вдруг, ваш исходный код был очень длинным, то можно после прохождения этапов сокращения первые 5 цифр оставить неизменными, а оставшиеся путем

суммирования привести к однозначному натуральному числу. Вариантов сокращения очень много. Экспериментируйте и выбирайте тот вариант, который Вам больше нравится.

Главное преимущество использования алгоритма шифрования, запомнив его, Вы всегда с легкостью сможете восстановить забытый код. И результат получается, на первый взгляд, максимально не связан с вашими данными, но поддающийся только вашей логике.

Заключение

В наше время шифры играют важную роль. Представьте жизнь без шифров! Все наши секреты перестанут быть секретами. Нашими ресурсами смогут воспользоваться другие люди. Жизнь станет небезопасной. Данная проблема очень актуальна, ведь криптография востребована повсеместно из-за потребности в сокрытии важных данных и информации от третьих лиц.

Это раньше мы использовали телефон только для звонков и СМС. Сейчас здесь хранится информации гораздо больше, а значит, появляется необходимость защиты своих данных. На каждый смартфон приходится десяток сервисов, нуждающихся в пароле. И обойтись отпиской в стиле «987654321» не получится — пароль либо отклонят на уровне системы, либо его взломают мошенники.

Практической значимостью данной работы является привлечение внимания к изучению проблем защиты информации в обществе. Результатом исследовательской работы является готовый продукт, а именно сборник основных видов шифрования, а также буклет, дающий рекомендации по созданию надежного пароля.

Подводя итоги нашему исследованию, можно сказать, что цель работы достигнута.

Список использованной литературы

1. http://ru.wikipedia.org
2. http://citforum.ru/security/cryptography/yaschenko/78.html
3. http://www.wikiznanie.ru/ru-wz/index.php/Шифр

4. «Книга шифров», Саймон Сингх
5. «Виды шифров», Алексей Банченко
6. https://habr.com/ru/post/444176/
7. https://dzen.ru/a/YEb3LkTtxmaBR9Kv