Государственное общеобразовательное учреждение

Лицей №150 Калининского района г. Санкт-Петербурга

Информационный проект

Криптография в нашем мире

Работу выполнила:  
Николайчук Валерия

Валентиновна   
Учащаяся 10 А класса  
Руководитель:  
Викулова Ирина Вадимовна,

учитель алгебры и геометрии

Санкт-Петербург

2023

**Содержание**

1.Паспорт проекта.

2.Введение

3.История криптографии.

4.Виды криптографии.

5.Самые известные виды шифров.

6.Криптография в нашей жизни.

7.Анкетирование.

8.Продукт проекта.

9.Заключение.

Словарь терминов и сокращений.

Список литературы.

Приложения.

**1.Паспорт проекта**

**Тема проекта.** Криптография в нашем мире.

**Тип проекта.** Информационный.

**Куратор проекта.** Викулова Ирина Вадимовна, учитель алгебры и геометрии ГБОУ Лицея №150.

**Противоречие.** В наши дни криптография стала не заменимой часть нашего существования, но многие люди не знают, что это такое и не понимают, для чего она нужна.

**Проблема**. Низкая степень осведомлённости общества о влиянии роли криптографии в их жизни.

**Продукт**: буклет об обеспечении конфиденциальности, целостности информации.

**Цель.** К концу 2022-2023 учебного года, увеличить информированность учащихся о безопасной передаче данных, тем самым обезопасить от взлома конфиденциальную информацию.

**Задачи.** Изучить историю криптографии с помощью различные источников информации; проанализировать литературу; изучить виды шифрования информации; провести опрос; подвести итоги; опубликовать буклет о криптографии на различных сайтах; разместить на школьном стенде.

**План реализации проекта** (« Дорожная карта»).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Этап | Задачи на этапе | Содержание работы | Прогнозируемый результат | Сроки |
| 1.Подготовительный | 1.Определить тему проекта, формы его организации.  2.Установить план действий и сформулировать задачи.  3.Сформулировать противоречие и проблему.  4.Перебрать варианты итогового продукта. | 1.Проанализировать наиболее актуальные темы для проектов и сформулировать цель.  2.Спланировать свою деятельность поэтапно, по срокам. | Утвердить тему проекта, тип и задачи. Грамотно составить противоречие и проблему. Определиться с продуктом. | Сентябрь-ноябрь. |
| 2.Основной | 1.Оперделить источники необходимой информации.  2.Создать продукт проекта. | 1.Собрать информацию из различных источников.  2.Офрмляю описание проекта.  3.Дорабатываю продукт проекта. | Найдены источники информации.  Создано описание проекта.  Сделан продукт проекта. | Декабрь-февраль. |
| 3.Аналитический | 1.Доработка проекта.  2.Консультация с куратором. | Корректировка материалов в случае необходимости. | Проект окончательно готов к размещению и защите. | Март - апрель. |
| 4.Заключительный | 1.Защита проекта | Публичная защита проекта в ГБОУ Лицее №150.Анализ публичной защиты. | Проект защищен. | Май. |

**SWOT-анализ** — метод стратегического планирования, заключающийся в

выявлении факторов внутренней и внешней среды организации и разделении

их на четыре категории: Strengths, Weaknesses, Opportunities, Threats.

|  |  |  |
| --- | --- | --- |
| внутренние | Strengths-сильные стороны:  1.Тема проекта является достаточно актуальной на данный момент;  2.Проект рассчитан на широкий круг лиц.  3.Малое количество аналогичных проектов. | Weaknesses-слабые стороны:  1.Скорость общественных изменений ограничена множеством интересов и стереотипами большого числа. |
| Внешние | Opportunities-возможности:  1.Привличение внимание к проблеме перехвата информации.  2.Развитие в сфере кодирования информации. | Threats-угрозы:  1.Не желание уделять внимание на решение данной проблемы. |

**2.Введение**

**Актуальность**. В современном мире постиндустриального общества, сопровождающегося информационной революцией, появляется острая необходимость в защите информации от её ложного содержания, подмены и использования в корыстных целях.

**Аналоговый анализ:**

|  |  |
| --- | --- |
| Название аналога | Сравнение |
| История криптографии в России https://znanio.ru/media/istoriya-kriptografii-v-rossii-2623202+ | Большое количество исторических данных.Нет видов криптографии, видов шифров. |
| Криптография  https://infourok.ru/issledovatelskaya-rabota-na-temu-kriptografiya-3688963.html | Много исторических данных, нет информации о криптографии в России. Нет исторических лиц, которые сделали вклад в криптографию. Есть виды шифров. |
| Криптографические способы шифрования информации https://урок.рф/library\_kids/issledovatelskaya\_rabota\_kriptograficheskie\_sposob\_185828.html | Большое количество исторических данных, но нет истории криптографии в России. Малое количество картинок Нет исторических лиц, которые сделали вклад в криптографию. |

**3**.**История криптографии.**

Первые профессиональные криптографы на Руси появились при Иване Грозном (1530–1584). Они находились на службе в Посольском приказе, созданном им в 1549 г. и отвечавшем за внешнюю политику страны. Криптографы разрабатывали так называемые «азбуки», «цифири», «цифры» или шифры, как они стали называться позднее. Сначала это были простые шифры замены. Первым из российских правителей, осознавшим всю важность криптографии для безопасности страны стал Петр I (1672–1725). Он поставил шифровальную службу действительно на профессиональную основу. С 1700 г. вся работа по созданию шифров, шифрованию и расшифрованию велась в цифирном отделении, а позднее в Посольской канцелярии. Криптографическая служба в это время находилась под постоянным и непосредственным контролем государственного канцлера.

Конец ХIХ века. 1879 год. Главный механик, помощник начальника Петербургского почтово-телеграфного округа Деревянкин разработал оригинальный прибор для шифрования телерамм **«Криптограф»** (шифровальный диск). Сам шифровальный диск представлял собой пару дисков, один из них вешний, неподвижный, второй -внутренний, подвижный. На внешнем были нанесены буквы в алфавитном порядке и цифры от 1 до 14; на внутреннем буквы были переставлены. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замену ее на соответственно находящуюся под ней букву шифрованного текста. После шифрования нескольких слов внутренний диск сдвигался на один шаг. Ключом служил порядок расположения букв на внутреннем диске и его начальное положение относительно внешнего диска. (Приложение 1)

Одним из первых аппаратов для шифрования была М-100 «Спектр». В 1937 году на ленинградском [заводе № 209 им. А. А. Кулакова](https://ru.wikipedia.org/w/index.php?title=%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BC%D0%B5%D1%85%D0%B0%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B7%D0%B0%D0%B2%D0%BE%D0%B4_%D0%B8%D0%BC%D0%B5%D0%BD%D0%B8_%D0%90._%D0%90._%D0%9A%D1%83%D0%BB%D0%B0%D0%BA%D0%BE%D0%B2%D0%B0&action=edit&redlink=1) были построены её первые опытные экземпляры (конструктор — [И. П. Волосок](https://ru.wikipedia.org/wiki/%D0%92%D0%BE%D0%BB%D0%BE%D1%81%D0%BE%D0%BA,_%D0%98%D0%B2%D0%B0%D0%BD_%D0%9F%D0%B0%D0%B2%D0%BB%D0%BE%D0%B2%D0%B8%D1%87)). Серийное производство началось на заводе в 1938 году. Использовалась эта машина до 1942 года, до последующей модернизации.

Модернизированная же версия, получившая название М-101 “Изумруд”. (Приложение 2)

**М-101 «Изумруд»** считался одним из самых криптографически стойких шифровальных устройств своего времени и использовался для обеспечения связи высшего звена управления стратегического уровня. Кроме того, «Изумруды» применялись в дальней бомбардировочной авиации. Известно, что в 1943 году в советские войска поставили 90 комплектов машин М-101.(Приложение 3)

**Влади́мир Алекса́ндрович Коте́льников** Выдающийся советский и российский учёный, инженер, педагог и организатор науки и образования, один из основоположников радиофизики, радиотехники, информатики, радиоастрономии и отечественной криптографии В суровые годы I Мировой войны, Октябрьской революции, Гражданской войны семья Котельникова переезжала из города в город, и его дальнейшее образование продолжалось самостоятельно по домашним книгам, а школьная учеба составила только 3 последних класса. Увлекаясь радиотехникой, Владимир в 1926 году поступил на электротехнический факультет МВТУ им. Н.Э. Баумана и одновременно посещал слушателем интересующие его курсы физико-математического факультета МГУ. В 1930 году по окончании электротехнического факультета Московского энергетического института , который в это время выделился из МВТУ, был принят на работу инженером в НИИ связи Красной армии. В 1931 году был зачислен в аспирантуру МЭИ, и одновременно последовательно работал лаборантом, ассистентом, доцентом, а также начальником лаборатории и главным инженером по радио в Центральном научно-исследовательском институте связи Народного комиссариата почт и телеграфов. Основные труды В. А. Котельникова посвящены проблемам совершенствования методов радиоприёма, изучению радиопомех и разработке методов борьбы с ними. К его крупнейшим научным достижениям, оказавшими существенное влияние на развитие мировой науки, следует отнести создание в 1933 году [теоремы отсчётов](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BE%D1%80%D0%B5%D0%BC%D0%B0_%D0%9A%D0%BE%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2%D0%B0), которая носит его имя и создание [теории потенциальной помехоустойчивости](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BE%D1%80%D0%B8%D1%8F_%D0%BF%D0%BE%D1%82%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9_%D0%BF%D0%BE%D0%BC%D0%B5%D1%85%D0%BE%D1%83%D1%81%D1%82%D0%BE%D0%B9%D1%87%D0%B8%D0%B2%D0%BE%D1%81%D1%82%D0%B8).(Приложение 4)

**4.Виды криптографии.**

Есть два основных типа шифрования: симметричное и асимметричное. Главное отличие между ними заключается в применении ключей.

В симметричном шифровании используется один ключ для шифрования и дешифрования данных. Такой ключ должен быть установлен на устройствах обоих собеседников. (Приложение 5)

Асимметричное шифрование — это метод шифрования данных, предполагающий использование двух ключей — открытого и закрытого. Открытый (публичный) ключ применяется для шифрования информации и может передаваться по незащищенным каналам. Закрытый (приватный) ключ применяется для расшифровки данных, зашифрованных открытым ключом. (Приложение 6)

**Хэширование.** Метод основывается на преобразовании исходной информации в байты заданного образца. Преобразование информации называется хэш-функцией, а полученный результат хэш-кодом (хэш текстом). Все хэш-коды имеют уникальную последовательность символов. (Приложение 7)

**Электронная подпись.** Это преобразование информации с использованием закрытого ключа, позволяющее подтвердить подлинность документа и отсутствие искажений данных.

**5.Самые известные виды шифров.**

1. Шифр Цезаря — это вид [шифра подстановки](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%BF%D0%BE%D0%B4%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B8), в котором каждый [символ](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%B2%D0%BE%D0%BB) в тексте заменяется символом, находящимся на некоторой позиции левее или правее него в [алфавите](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D1%84%D0%B0%D0%B2%D0%B8%D1%82). Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

2. Шифр транспонирования .В транспозиционном шифре буквы переставляются по заранее определённому правилу. Например, если каждое слово пишется задом наперед, то из ПРИВЕТ получается ТЕВИРП

3. Азбука Морзе. В азбуке Морзе каждая буква алфавита, цифры и наиболее важные знаки препинания имеют свой код, состоящий из череды коротких и длинных сигналов. Чаще всего это шифрование передаётся световыми или звуковыми сигналами. (Приложение 8)

4.Шифр Энигмы.Энигма —  переносная [шифровальная машина](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%B0%D1%82%D0%BE%D1%80_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)), использовавшаяся для [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) и расшифрования секретных сообщений, Есть несколько колёс и клавиатура. На экране оператору показывалась буква, которой шифровалась соответствующая буква на клавиатуре. То, какой будет зашифрованная буква, зависело от начальной конфигурации колес. Существовало более ста триллионов возможных комбинаций колёс, и со временем набора текста колеса сдвигались сами, так что шифр менялся на протяжении всего сообщения. (Приложение 9)

5. Текстовые данные вполне можно хранить и передавать в двоичном коде. В этом случае по таблице символов каждое простое число сопоставляется с буквой: 01100001 = 97 = «a», 01100010 = 98 = «б» и т.д.

**6.Криптография в нашей жизни.**

Изначально криптография использовалась правительством для безопасного хранения или передачи документов. Современные же асимметричные алгоритмы шифрования получили более широкое применение в сфере IT-безопасности, а симметричные методы сейчас применяются преимущественно для предотвращения несанкционированного доступа к информации во время хранения.

Почти любое соединение с сайтом или сервисом в сети интернет происходит на фоне интенсивного обмена зашифрованными данными, открытыми ключами, сертификатами, множественными запросами и ответами на них. Вся эта бурная деятельность не видна глазу, но очень важна и скрывает в себе сложные криптографические процессы.

Чтобы предоставить пользователю доступ в его виртуальный аккаунт, система проводит аутентификацию его личности, например, с помощью пароля или биометрии путем сканирования отпечатка пальца или сетчатки глаза. Авторство документов проверяется с помощью цифровых подписей, которые подобны электронным «отпечаткам пальцев». В форме закодированного сообщения цифровая подпись связывает автора с документом.

**7. Анкетирование**

Я провела анкетирования на знание криптографии, в котором участникам нужно было ответить на вопросы.

Участвовало 40 человек.

Вопросы анкеты

1.Что такое криптография?

2.Каких известных криптографов вы можете назвать?

3. Какие есть виды криптографии?

4. Где используется криптография?

5. При ком впервые появилась криптография в России?

6.Важна ли криптография в современном мире?

(Приложение 10)

**8.Продукт проекта**

**Проведя опрос, я поняла, что многие не знают, что такое криптография и где она применяется. Я решила сделать брошюрку, которая поможет узнать больше о криптографии в современном мире.**

**(Приложение 11)**

**9.Заключение.**

С целью увеличения информированности учащихся о безопасной передаче данных в ближайшей перспективе необходимо опубликовать буклет о криптографии на различных сайтах и на стенде в школе. Выполнение этих шагов позволит повысить заинтересованность (интерес) обучающихся, как следствие, поможет решить проблемы низкой осведомленности учащихся и пренебрежением защиты данных. Однако, эти проблемы необходимо решать в комплексе с активным участием образовательных, государственных и частных учреждений, поскольку для реализации подобной концепции требуются определённые затраты времени, финансов и умственных ресурсов.

**Словарь терминов**

**Криптогра́фия** — наука о методах обеспечения конфиденциальности, целостности данных. То есть благодаря криптографии наши персональные данные защищены от возможной кражи и могут участвовать в безопасной передаче информации в Интернете.

**Криптоло́гия** — наука, занимающаяся методами [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) и [дешифровки](https://ru.wikipedia.org/w/index.php?title=%D0%94%D0%B5%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BA%D0%B8&action=edit&redlink=1). Криптология состоит из двух частей — [криптографии](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) и [криптоанализа](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7" \o "Криптоанализ). Криптография занимается разработкой методов шифрования данных, в то время как криптоанализ занимается оценкой сильных и слабых сторон методов шифрования, а также разработкой методов, позволяющих взламывать [криптосистемы](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80).

**Криптоана́лиз**— наука о методах [дешифровки](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F#%D0%A2%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F) зашифрованной информации без предназначенного для этого [ключа](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)), а также сам процесс такой дешифровки.

**Радиоастроно́мия** — раздел [астрономии](https://ru.wikipedia.org/wiki/%D0%90%D1%81%D1%82%D1%80%D0%BE%D0%BD%D0%BE%D0%BC%D0%B8%D1%8F), изучающий [космические объекты](https://ru.wikipedia.org/w/index.php?title=%D0%9A%D0%BE%D1%81%D0%BC%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D0%BE%D0%B1%D1%8A%D0%B5%D0%BA%D1%82%D1%8B&action=edit&redlink=1) путём исследования их [электромагнитного излучения](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BC%D0%B0%D0%B3%D0%BD%D0%B8%D1%82%D0%BD%D0%BE%D0%B5_%D0%B8%D0%B7%D0%BB%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) в [диапазоне](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D0%B0%D0%BF%D0%B0%D0%B7%D0%BE%D0%BD_%D1%87%D0%B0%D1%81%D1%82%D0%BE%D1%82) [радиоволн](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D0%B8%D0%BE%D0%B2%D0%BE%D0%BB%D0%BD%D1%8B).**[МГУ](http://www.bmstu.ru/" \t "_blank)** [- Московский государственный университет имени](http://www.bmstu.ru/" \t "_blank) [[Михаила Васильевича](http://www.bmstu.ru/" \t "_blank)](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BC%D0%BE%D0%BD%D0%BE%D1%81%D0%BE%D0%B2,_%D0%9C%D0%B8%D1%85%D0%B0%D0%B8%D0%BB_%D0%92%D0%B0%D1%81%D0%B8%D0%BB%D1%8C%D0%B5%D0%B2%D0%B8%D1%87)[Ломоносова](http://www.bmstu.ru/" \t "_blank)

**МВТУ** -Моско́вский госуда́рственный техни́ческий университе́т им. [Николая Эрнестовича](https://ru.wikipedia.org/wiki/%D0%91%D0%B0%D1%83%D0%BC%D0%B0%D0%BD,_%D0%9D%D0%B8%D0%BA%D0%BE%D0%BB%D0%B0%D0%B9_%D0%AD%D1%80%D0%BD%D0%B5%D1%81%D1%82%D0%BE%D0%B2%D0%B8%D1%87) Ба́умана

**МЭИ**-Московский энергетический институт

**Доце́нт**— [учёное звание](https://ru.wikipedia.org/wiki/%D0%A3%D1%87%D1%91%D0%BD%D0%BE%D0%B5_%D0%B7%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) преподавателей [высших учебных заведений](https://ru.wikipedia.org/wiki/%D0%92%D1%8B%D1%81%D1%88%D0%B5%D0%B5_%D1%83%D1%87%D0%B5%D0%B1%D0%BD%D0%BE%D0%B5_%D0%B7%D0%B0%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5)

**НИИ** -Научно-испытательный институт

**Аутентификация**— это основа безопасности любой системы, которая заключается в проверке подлинности данных о пользователе сервером.

**Список литературы.**

<file:///C:/Users/пк/Downloads/ob-istorii-kriptografii-v-rossii.pdf>

<https://opartnerke.ru/chto-takoe-shifrovanie-vidy-algoritmy/>

<https://ru.wikipedia.org/wiki/Криптография>

[https://ru.wikipedia.org/wiki/М-100\_«Спектр»](https://ru.wikipedia.org/wiki/М-100_)

<https://georgy-bat.livejournal.com/31121.htm>

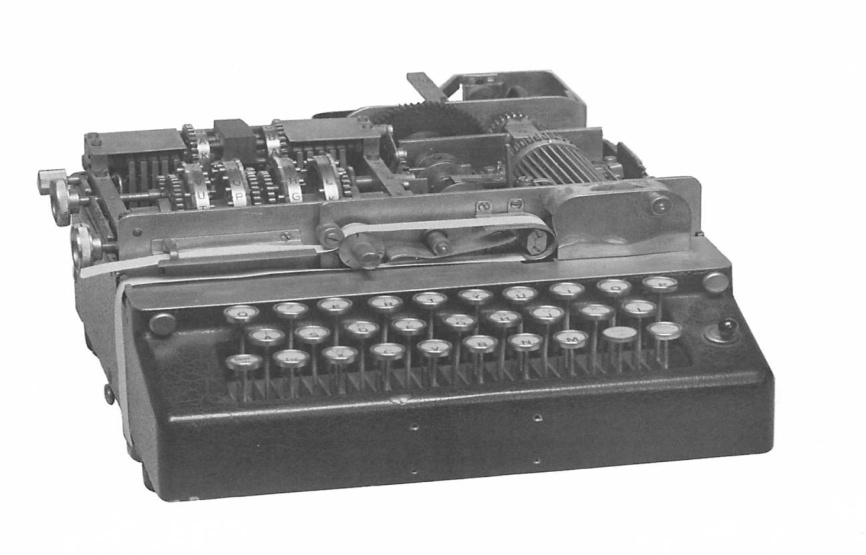
<https://ru.wikipedia.org/wiki/Котельников,_Владимир_Александрович>

<https://habr.com/ru/company/ua-hosting/blog/368663/>

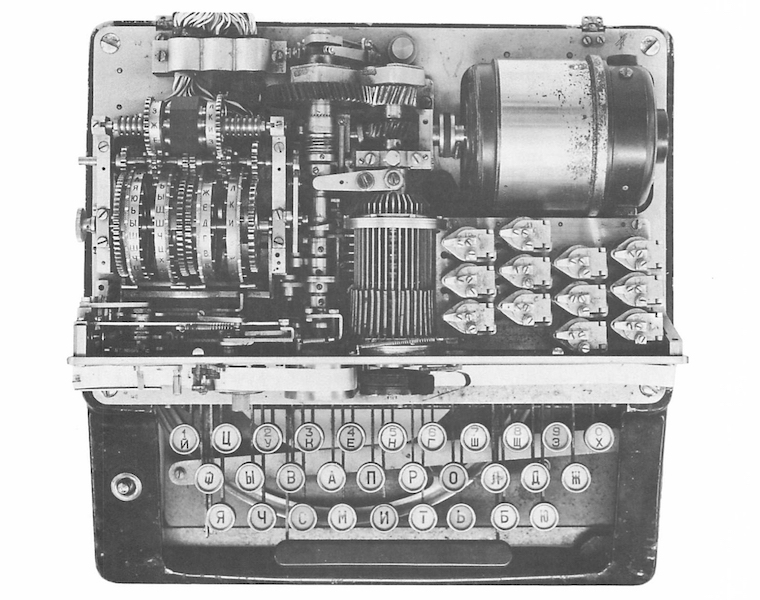
**Приложение 1**. **«**Криптограф» (шифровальный диск).



**Приложение 2**. М-100 «Спектр».



Приложение 3. М-101 «Изумруд» .



**Приложение 4**. Влади́мир Алекса́ндрович Коте́льников.



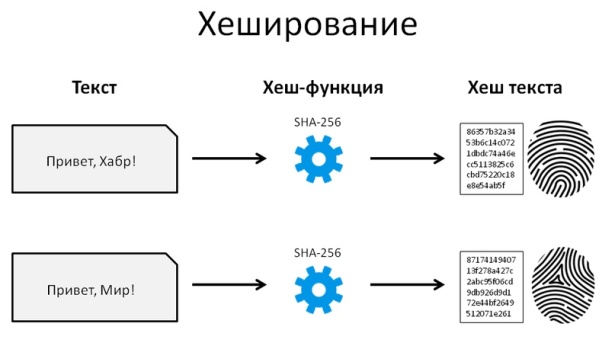
**Приложение 5**. Симметричное шифрование.



**Приложение 6**. Асимметричное шифрование.



**Приложение 7**. Хэширование.



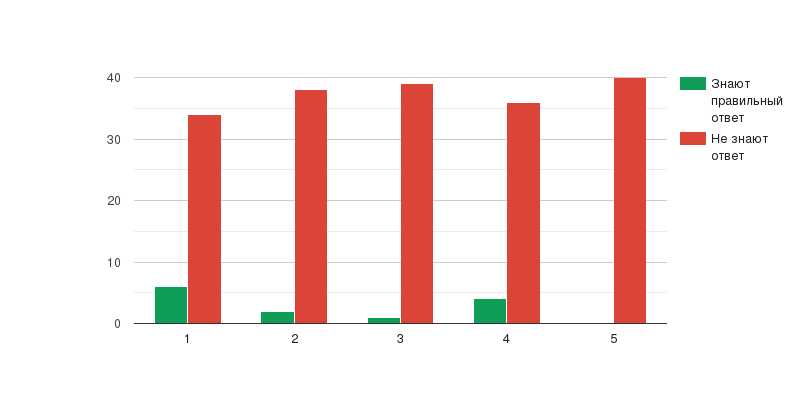
**Приложение 8**. Азбука Морзе



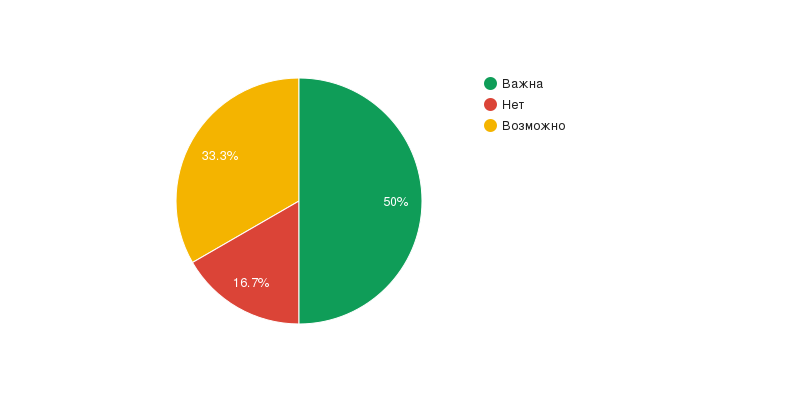
**Приложение 9**. Энигма.



**Приложение 10**. Результаты анкетирования.



6.



**Приложение 11**.Продукт проекта.



