УДК 004.5: 003.26 **Информационные технологии**

Базеева Наталья Алексеевна, *преподаватель факультета довузовской подготовки и среднего профессионального образования, ФГБОУ ВО «Мордовский государственный университет им. Н.П. Огарёва»*

Ушакова Екатерина Евгеньевна, *студентка факультета довузовской подготовкии среднего профессионального образования, ФГБОУ ВО «Мордовский государственный университет им. Н.П. Огарёва»*

КРИПТОГРАФИЯ. ЕЕ ОСНОВОПОЛАГАЮЩИЕ МЕТОДЫ, РАЗВИТИЕ И ПЕРСПЕКТИВЫ

Аннотация: В материале рассматриваются основные методы криптографии и раскрыто их содержание. Работа содержит поэтапное развитие криптографии по истечению веков. Также уделяется внимание актуальности данной науки в современности.

Ключевые слова: криптография, методы криптографии, стенография, кодирование, сжатие шифрование.

Abstract: The article discusses the main methods of cryptography and reveals their content. The work contains a step-by-step development of cryptography over the centuries. Attention is also paid to the relevance of this science in modern times.

Keywords: cryptography, cryptographic methods, shorthand, encoding, compression, encryption.

Слово, связанное с секретами, «криптография» имеет удивительно прозрачную этимологию. Это слово восходит к греческим корням kryptos (От греч. κρυπτός), что означает «скрытый», и graphein (От греч. Γράμμα), что означает «писать».

Криптография, как наука направлена на решение двух главных задач, это — обеспечение конфиденциальности и целостности информации. Решение этих задач происходит через различные методы, цель которых — преобразовать данные таким образом, чтобы они не представляли ценности для злоумышленников. На данный момент можно выделить основными следующие методы криптографии:

- стенография,
- кодирование,
- сжатие
- шифрование.

В интернете шифрование представляет собой незаменимый инструмент, использующийся в качестве защиты информации. Шифрованием достигают следующей цели: приведение информации в хаотичный вид, невозможного для чтения набора символов, букв и цифр. Однако, данный процесс имеет обратное действие, при условии, что у оператора имеются: алгоритм преобразования, ключ дешифровки, а также исходные данные.

Стенография несколько отличается от остальных методов криптографии, так как дает возможность сохранить в тайне не только смысл, но и само обстоятельство передачи и хранения закрытой информации. Как метод, стенография основывается на маскировке файлов с закрытыми данными, среди открытых файлов. В итоге сокрытия секретных данных и формирования реалистичных — их становится невозможно отличить друг от друга. При этом, скрытый файл также может быть и зашифрован и если кто-то его обнаружит - воспримет это как сбой в работе системы [1]. Совместное использование данных методов: шифрование+стенография, значительно снижает риск обнаружения и "прочтения" секретной информации.

При следующем методе — **кодировании**, совершается преобразование данных в форму кода. В таком случае код может быть представлен цифрами, знаками или сочетаниями букв. В случае использовании этого метода криптографии понадобятся специальные словари и таблицы. В настоящий

момент кодирование используют и информационные сети, преобразовывая начальное сообщение программно-аппаратными средствами, в процессе чего возрастает достоверность информации, которую мы хотим передать. Кодирование и шифрование — это два разных метода, хотя возможно с первого взгляда так и не скажешь и их часто путают. Отличие состоит в том, что если необходимо восстановить информацию, которая была закодирована — оператор должен иметь алгоритм замены. А при использовании шифрования, нам нужно будет знать правила шифровая и сам ключ.

Третий метод упоминают не все источники и возможно его добавление спорно, но все же требует рассмотрения, так он часто используется в совокупности с шифрованием. Мы говорим о **сжатии** информации, цель которого уменьшить занимаемый объем информации (данных). В этом случае, доступ к информации может быть получен только путем обратного преобразования. В настоящее время, сжатие и обратное преобразование крайне доступно, даже при условии, что алгоритм является секретным. Они имеют достаточно большую вероятность быть раскрытыми методом подбора и на основании собранной статистики. Поэтому при сжатии конфиденциальной информации следующим этапом идет ее шифрование. Сжатие же в данном случае экономит наше время при передаче данных.

Защита информации всегда была важной целью, об этом свидетельствуют множество источников и некоторым из них. 4 тысячи лет.

В древности криптографию использовали для сохранения секретности сообщений, после того как появилась письменность. Хотя и само изобретение письма, в некоторой мере представляло собой криптографию - из-за небольшого количества образованных людей. Но со временем этот круг начал расширяться. В древнем мире были достаточно примитивные методы, которые сейчас можно косвенно отнести к криптографии. Например, в Древнем Египте, 4 тысячи лет назад использовали специальные иероглифы (это первое упоминание в истории). Вот только у египтян тогда стояла задача не скрыть

информацию или усложнить чтение, а соревнование в красноречии и изобретательности. Это был способ привлечения внимания к текстам.

Еще одно упоминание - это изобретение устройства под названием Сциталла. Один из древнейших механизмов криптографии известный миру (примерно 400 года до нашей эры), он же — "шифр древней Спарты". Как же выглядело устройство? Оно представляло из себя палку(стержень), на который нужно было наматывать пергамент в виде ленты. Таким образом, намотав ленту по спирали, получали площадь для письма. Текст записывали по длине стержня, после чего пергамент снимали и передавали получателю. В виде размотанной ленты тест был нечитаемым. А чтобы прочитать сообщение, требовался стержень, который бы совпадал с изначальным диаметром. Позже Аристотель раскрыл шифр Сциталлы, взяв за основу конус, он наматывал пергамент с текстом, меняя высоту. Таким образом подбирая необходимый диаметр. После чего, сообщение становилось доступным для чтения.

Возможно, самый яркий пример криптографии Древнего Мира — это Шифр Цезаря. Это достижение римской криптографии заключалось в определенном методе подстановки, где каждый символ в тексте подменяется символом, который располагается на постоянном удалении от него. Как правее, так и левее.

В Средние Века и Эпоху Возрождения криптография как формируется как наука, становится сложнее. Хотя шифр Цезаря все же остается стандартом. Пожалуй наиболее яркий пример того времени — это арабский математик Аль-Кинди. Который разработал метод частотного анализа (около 800 г. н.э.). Этот подход позволял расшифровывать сообщения, основываясь на систематическом методе. Ученый брал за основу метод математической статистики, подмечая закономерности в алфавите.

Также ученый, работу которого хотелось бы рассмотреть — это Леоне Альберти. В 1465 году году он представил полиалфавитный шифр. Суть этого метода заключается в шифровании, с помощью двух разных алфавитов. На первом мы пишем сообщение, а на втором алфавите появляется сообщение

после кодирования. Шифрование осуществлялось при использовании специального диска. Использование полиалфавитных шифров совместно с шифрами заменяющими, позволяло существенно повысить безопасность сообщения.

Следующий этап пришелся на промышленную революцию, его можно смело назвать эрой шифровальных машин. Криптографию не обошла стороной автоматизация, для шифрования применялись роторные криптосистемы. Одним из самых заметных изобретений Нового времени (около 1790 г), была механическая машина Томаса Джефферсона, ее еще называли цилиндром Джефферсона. А в 1917 Эдвард Хеберн создал Enigma, которую после доработал Артур Кирх. Роторные системы активно использовались по время второй мировой войны, позволяя создавать очень устойчивые шифры.

Подытоживая, можно смело утверждать, что ранее криптография использовалась политиками, военными и дипломатам, а создавали ее ученые, которые на протяжении многих веков засекречивали данные вручную. Да, конечно в наше время появились шифровальные машины, но все же сфера криптографии была ограничена кругом посвященных лиц.

Изобретение компьютера и создание доступного интернета — вот что дало возможность стать криптографии более доступной. Например, сюда можно отнести сотовую связь, защиту электронного почтового ящика от спама, банковские операции, цифровое ТВ и много другое. Ее стали применять частные лица в электронных коммерческих операциях, так и бизнес. В следствии чего у нас появилась валюта под названием биткойн, эта валюта не подконтрольна государству. Были созданы технологии, для транзакций криптовалют — блокчейн.

Можно сказать, что одно из последних применений криптографии — это Data Matrix-коды. Таким образом борются с подделками, маркируя товары. Эти коды состоят из кода индентификации и криптохвоста. Таки образом, у нас есть система маркировки, которая генерирует код. Он уникальный, в нем содержатся данные о товаре, он определяет позицию товара в системе и едином

каталоге, а криптохвосты дополнительно шифруют каждый код на производстве. Так как в системе нет сохраненного целиком кода, воссоздать его не предоставляется возможным. К тому же, система минимум 5 лет, не будет его перевыпускать, с даты выпуска товарной позиции [3].

Стремительное развитие технологий в сфере компьютеров привело к тому, что криптография перешла к сложным алгоритмам шифрования. А с появлением мобильной связи, устройств и интернета вывело ее в гражданское поле. Еще одна сторона криптографии, которую хотелось бы рассмотреть — юридическая, а именно — государственное регулирование.

В вопросе регулирования есть две заинтересованные стороны — это собственно государство, которое желает сохранить секретность и борцы за гражданские права, коммерческие структуры.

Правозащитники основываются на 12 Всеобщей декларации прав человека (ООН 1948 г.): «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту от такого вмешательства или таких посягательств» [2].

На данный момент для граждан именно шифрование остается главным гарантом прав на личную жизнь. Со стороны бизнеса же интерес в шифровании онлайн сферы, развития электронной коммерции, как результат — возможности успешного ведения бизнеса, без опасений что данные поставщиков окажутся в открытом доступе или попадут в чужие руки.

Библиографический список:

1. Криптографические методы защиты информации [Электронный ресурс] «ИНТУИТ» Национальный открытый университет — Режим доступа:https://intuit.ru/studies/courses/16655/1300/lecture/25505?page=2.

2. Правовое регулирование шифрования онлайн-коммуникаций [Электронный ресурс] Центр цифровых прав — Режим доступа:

https://digitalrights.center/blog/pravovoe-regulirovanie-shifrovaniya-onlayn-kommunikatsiy/.

3. Современная криптография: заботы спецслужб и инструменты для бизнеса [Электронный ресурс] Naked Science — Режим доступа: https://naked-science.ru/article/sci/sovremennaya-kriptografiya-zaboty.