УДК 51-77

94. МЕТОДЫ ШИФРОВАНИЯ И КОДИРОВАНИЯ И ИХ ПРИМЕНЕНИЕ В СФЕРЕ МАРКЕТИНГА

Резникова Д.М., Матяс П.Д., студенты гр. 477601

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Русина Н. В. – ст. преп., каф. ЭИ

Аннотация: В данной работе рассматриваются методы шифрования и кодирования информации и их применение в сфере маркетинга. Криптография, как метод безопасной передачи информации, играет ключевую роль в обеспечении защиты личных данных клиентов, особенно в контексте использования CRM-систем. В статье подробно анализируются симметричные алгоритмы шифрования, такие как AES, и методы сквозного шифрования (E2EE), которые обеспечивают надежную защиту информации в электронной коммерции. Также рассматриваются возможности применения шифрования в рекламных кампаниях, включая использование простых шифров, таких как шифр Цезаря и шифр Виженера, для создания интерактивного взаимодействия с потребителями. Работа подчеркивает важность шифрования как инструмента для формирования доверительных отношений между компаниями и клиентами, а также для защиты их личной информации в условиях растущих киберугроз.

Ключевые слова: криптография, шифрование, AES, сквозное шифрование, маркетинг, CRM-системы, безопасность данных, симметричное шифрование, ассиметричное шифрование.

Стремительно развивающиеся в современном обществе информационные технологии неминуемо приводят к образованию потребности в конфиденциальности, защите и обеспечении целостности информации. В настоящее время криптография используются для сохранности данных не только государства, но и частных лиц, и организаций. Механизмы и средства шифрования применяются в различных современных областях, в том числе и при реализации маркетинговой деятельности. В данной статье будет рассмотрена тема методов шифрования и кодирования и их применение в сфере маркетинга. Мы рассмотрим основные принципы работы симметричных и сквозных алгоритмов шифрования, используемых для обеспечения цифровой безопасности в электронной коммерции.

Криптография – это метод сокрытия или шифрования данных, прочитать которые сможет только адресат, у которого есть ключ к шифру. Термин происходит от сочетания двух греческих слов: kryptós – «тайный» и grapho – «пишу». При буквальном переводе с греческого слово «криптография» означает «тайнопись», но на самом деле под этим термином понимается безопасная передача информации [1].

В основе задач криптографии лежит обеспечение конфиденциальности данных, для решения которой применяется шифрование данных.

Шифрование — процесс применения шифра к защищаемой информации, т. е. преобразование защищаемой информации (открытого текста) в шифрованное сообщение (шифртекст, криптограмму) с помощью определенных правил, содержащихся в шифре [2].

Каждый шифр определяется некоторым параметром, называющийся ключом. Под ключом в данных методах понимают сменный элемент шифра, который применяется для шифрования [3].

В настоящее время маркетинг направлен на таргетированную аудиторию, что привело к появлению такого инструмента как CRM (Customer Relationship Management), который работает на улучшении качества обслуживания и повышает эффективность работы с помощью автоматизированных процессов.

CRM система - это программное обеспечение, которое позволяет автоматизировать все взаимодействия с клиентами, управлять продажами, маркетингом и обслуживанием клиентов. Защита личной информации клиентов в CRM-системе играет ключевую роль, поэтому применение шифрования становится важным элементом этого процесса. Чаще всего используется такой метод как AES (Advanced Encryption Standart) шифрование, относящийся к симметричным алгоритмам шифрования.

Симметричное шифрование - это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации.

Благодаря технологии AES-шифрования данные пользователей надёжно защищены, что гарантирует их конфиденциальность и защиту от мошенников.

Данный метод шифрования широко применяется в использовании по следующим причинам:

1) Сложность расшифровки ключа, что, соответственно, предотвращает несанкционированный доступ, кибератаки и кражи.

2) AES сертифицирован Национальным институтом стандартов и технологий США в 2001 году. Кроме этого, алгоритм был признан самым безопасным на международном уровне.

3) Высокая скорость обращения данных.

На рисунке 1 представлены данные о статистике эффективности метода AES, демонстрирующие его высокую производительность и надежность в сравнении с другими методами шифрования.

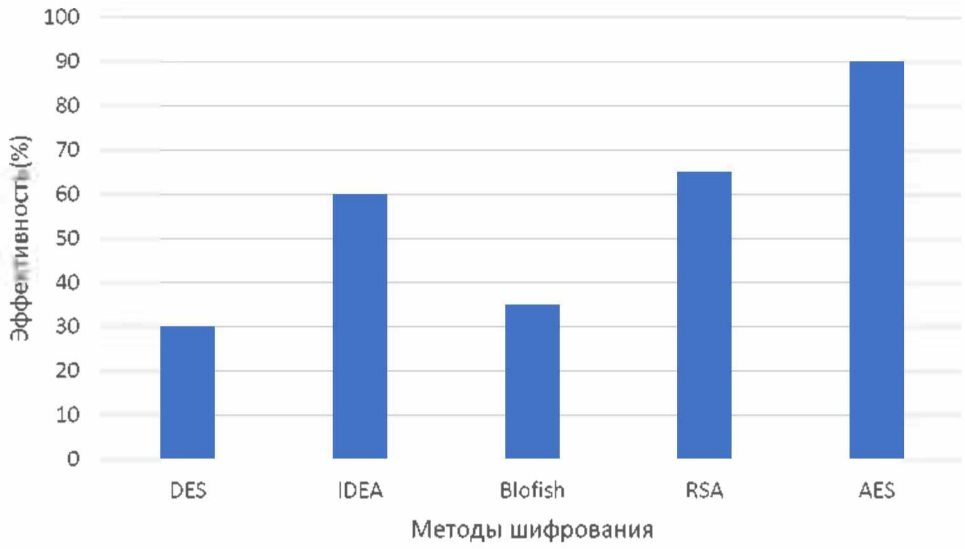

Рисунок 1 – Эффективность алгоритма шифрования AES (в %)

Одним из, безусловно, важнейших методов шифрования является сквозное шифрование (также известное как оконечное шифрование, end-to-end encryption или E2EE) —метод защиты данных от несанкционированного просмотра и изменения, при котором доступ к сообщениям или данным имеют только те пользователи, которые участвуют в общении. Данный метод может быть реализован как с использованием симметричных, так и ассиметричных алгоритмов шифрования.

Асимметричные алгоритмы — это алгоритмы, которые используют два различных ключа: открытый и закрытый. Открытый ключ может быть свободно распространен, в то время как закрытый ключ известен только владельцу. Это позволяет любому пользователю отправить сообщение, зашифрованное открытым ключом, который может быть расшифрован только закрытым ключом.

Сквозное шифрование обеспечивает надежную защиту пользовательской информации от доступа, включая серверы, участвующие в передаче данных. Процесс шифрования осуществляется исключительно на устройствах пользователей, которые задействованы в разговоре, что гарантирует, что только получатель сможет прочесть или изменить передаваемые данные.

Принцип работы метода состоит в том, что при создании сеанса связи приложение-получатель генерирует два ключа: публичный и закрытый. Публичный ключ отправляется на сервер и используется исключительно для шифрования, что не позволяет серверу прочитать сообщение отправителя. Важно удостовериться, что сервер принадлежит надежному поставщику, чтобы исключить возможность атаки MITM (человек-по-середине, man-in-the-middle, атака посредника) и не допустить подмены ключей. Приложение-отправитель загружает с сервера публичный ключ, с его помощью шифрует сообщение и отправляет его на сервер. Затем приложение-получатель скачивает зашифрованное сообщение и расшифровывает его с помощью своего закрытого ключа [4].

Маркетинг, особенно цифровой, часто основывается на данных клиентов, таких как предпочтения, истории покупок, демографическая информация и т.д., поэтому важную роль играет сохранность информации при передаче ее через каналы коммуникации как мобильные устройства и мессенджеры. Если компания взаимодействует с покупателями онлайн через консультанта в сообщениях или чат-боты, то благодаря наличию данного метода шифрования вся личная информация клиентов, предоставленная в ходе общения, будет защищена и строго конфиденциальна.

Как показано в таблице 1, метод сквозного шифрования (End-to-End Encryption) обеспечивает защиту данных на всех этапах их передачи и хранения.

В отличие от метода шифрования "hop-by-hop", сквозное шифрование обеспечивает все те же возможности, что и шифрование по принципу «хоп-хоп», но со значительными дополнительными гарантиями. Прежде всего, оно устраняет повсеместный пробел в конфиденциальности, присущий шифрованию по принципу «хоп-хоп», защищая пользовательские данные от атак на вычислительные ресурсы. Во-вторых, она служит примером принципа наименьших привилегий (POLP), предоставляя криптографические средства для ограничения доступа к пользовательским данным только тем, кто имеет явные полномочия. Сочетание шифрования по принципу «хоп-хоп» и сквозного шифрования обеспечивает глубинную защиту (Defense in Depth, DiD), когда успешная атака на одном уровне может быть смягчена другим.

Strategy	Network	Storage	Compute	POLP	DiD
Hop-by-Hop Encryption	secure	secure	not secure	no	no
End-to-End Encryption	secure	secure	secure	yes	yes

Таблица 1 – Сравнение методов шифрования по уровню безопасности

Помимо этого, методы шифрования можно использовать и в рекламе. Для представления своих новых продуктов бренды могут организовывать рекламные кампании, в которых зашифрованное сообщение подается в виде тизера. В настоящее время широко распространены в массах шифры, такие как шифр Цезаря или шифр Виженера.

Шифр Цезаря – это один из самых простых и широко известных методов шифрования, который был использован уже в древности. Он основан на замене каждой буквы в сообщении на другую букву, находящуюся на фиксированное число позиций в алфавите.

Шифр Виженера был разработан в XVI веке благодаря итальянскому дипломату Блезу де Виженеру. Этот шифр является полиалфавитным шифром замены, то есть каждая буква сообщения заменяется на другую букву, зависящая от позиции символа в сообщении и ключа шифрования [5].

В заключении, алгоритмы шифрования являются основополагающим инструментом не только в области информационных технологий и защиты авторских прав на интеллектуальную собственность, но и открывают новые возможности для маркетинга, позволяя компаниям строить доверительные отношения с клиентами и обеспечивать безопасность их личной информации. Использование таких методов, как симметричное шифрование (например, AES) и сквозное шифрование (E2EE), позволяет организациям эффективно защищать данные пользователей, что особенно важно в условиях растущих угроз кибербезопасности.

Кроме того, шифрование может быть интегрировано в маркетинговые стратегии, создавая интерактивные и увлекательные способы взаимодействия с аудиторией. Применение шифров, таких как шифр Цезаря или Виженера, может не только привлечь внимание потребителей, но и повысить интерес к продуктам.

Список использованных источников:

1. Что такое криптография? [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-cryptography – Дата доступа: 30.03.2025.

2. Шифрование [Электронный ресурс] – Режим доступа: https://studfile.net/preview/5947521/page:2/ – Дата доступа: 30.03.2025.

3. Алфёров, А. П., Зубов, А. Ю., Кузьмин, А. С., Черемушкин, А. В. Основы криптографии : учеб. пособие / А. П. Алфёров, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – Москва: "Гелиос АРВ", 2002. – 54 с.

4. Сквозное шифрование(E2EE) [Электронный ресурс] – Режим доступа: https://trueconf.ru/blog/wiki/skvoznoe-shifrovanie-e2ee – Дата доступа: 30.03.2025.

5. Вульф А., Криптография. Основы практического шифрования и криптографии / Вульф А. - Екатеринбург: ООО "Издательские решения", 2023. - 7 с.

UDC 51-77

ENCRYPTION AND CODING METHODS AND THEIR APPLICATION IN THE SPHERE OF MARKETING

Reznikova D.M., student of group 477601, Matyas P.D., student of group 477601

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Rusina N. V. - Senior Lecturer of the Department of EI

Annotation: This paper aims to examine the methods of encryption and coding of information and their application in the field of marketing. Cryptography, as a method of secure information transmission, plays a key role in ensuring the protection of customers' personal data, especially in the context of using CRM-systems. This study analyzes symmetric encryption algorithms such as AES and end-to-end encryption (E2EE) methods that provide strong information security in e-commerce. The application of encryption in advertising campaigns is also discussed, including the use of simple ciphers such as the Caesar cipher and the Vigenère cipher to create an interactive experience with consumers. The paper emphasizes the importance of encryption as a tool for building trust between companies and customers, as well as protecting their personal information in the face of growing cyber threats.

Keywords: cryptography, encryption, AES, end-to-end encryption, marketing, CRM systems, data security, symmetric encryption, asymmetric encryption