Удальцов К.Р. Значение конечного шифрования для защиты конфиденциальности данных // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 5(43) с. 56–59

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ЗНАЧЕНИЕ КОНЕЧНОГО ШИФРОВАНИЯ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ

Удальцов К.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: 2003.06.10kr@gmail.com

Данная статья обсуждает важность конечного шифрования (End-to-End Encryption, E2EE) в контексте защиты конфиденциальности данных. Автор рассматривает преимущества этого метода шифрования, его роль в обеспечении частной жизни, а также значение в сфере бизнеса. Также освещаются вызовы, с которыми сталкивается конечное шифрование, и перспективы его развития в будущем. Статья предназначена для широкой аудитории, включая индивидуальных пользователей, компании и специалистов в области кибербезопасности, а также всех, кто интересуется защитой данных в цифровой эпохе.

Ключевые слова: Конечное шифрование, защита данных, конфиденциальность, кибербезопасность, E2EE, цифровая безопасность, шифрование, приватность, бизнес-сфера, обмен сообщениями, информационная безопасность.

THE VALUE OF END-TO-END ENCRYPTION TO PROTECT DATA PRIVACY

Udaltsov K.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: 2003.06.10kr@gmail.com

This article discusses the importance of End-to-End Encryption (E2EE) in the context of data privacy protection. The author examines the advantages of this encryption method, its role in ensuring privacy, as well as its importance in the business sphere. It also highlights the challenges faced by end-to-end encryption and the prospects for its development in the future. The article is intended for a wide audience, including individual users, companies and cybersecurity professionals, as well as anyone interested in data protection in the digital age.

Keywords: end encryption, data protection, privacy, cybersecurity, E2EE, digital security, encryption, privacy, business sphere, messaging, information security.

Введение

В современном мире, где информация стала ключевым ресурсом, защита данных и обеспечение их конфиденциальности стали важнейшими задачами. Одним из наиболее надежных методов защиты конфиденциальности данных является конечное шифрование. Этот метод шифрования играет критическую роль в предотвращении несанкционированного доступа к чувствительной информации.

1. Что такое конечное шифрование?

Конечное шифрование (End-to-End Encryption, E2EE) [1] - это способ шифрования данных, который позволяет отправителю и получателю обмениваться информацией, которая остается зашифрованной на всех этапах передачи, а расшифровать её может только предполагаемый получатель. Даже поставщик услуги обмена сообщениями или хранения данных не имеет возможности прочитать содержимое сообщений.

2. Защита от несанкционированного доступа

Одним из ключевых преимуществ конечного шифрования является его способность предотвращать несанкционированный доступ к данным. [1] Благодаря этому методу шифрования, данные остаются защищенными на всех этапах передачи и хранения, что делает практически невозможным их расшифровку третьими лицами без соответствующих ключей.[2]

3. Защита конфиденциальности в цифровых коммуникациях

В сфере цифровых коммуникаций конечное шифрование становится все более важным. [2] При обмене сообщениями через различные платформы, где конфиденциальность имеет первостепенное значение, использование конечного шифрования обеспечивает надежную защиту от перехвата сообщений третьими лицами.

4. Преимущества конечного шифрования [3]

Конечное шифрование обладает неоспоримыми преимуществами, особенно в контексте сохранения конфиденциальности данных. [4] Одним из ключевых аспектов является то, что даже сам провайдер услуги обмена сообщениями или хранения данных не имеет доступа к содержимому сообщений, поскольку оно остается зашифрованным на всех этапах передачи. Это создает непреодолимый барьер для злоумышленников, предотвращая утечку конфиденциальной информации.

5. Значение в сфере бизнеса

В бизнес-среде конечное шифрование становится важным инструментом для защиты коммерческих тайн, финансовой информации и персональных данных клиентов. [3] Благодаря этому методу шифрования компании могут обмениваться конфиденциальной информацией, будучи уверенными в её безопасности, что способствует поддержанию доверия клиентов и партнёров.[5]

6. Вызовы и перспективы

Несмотря на все преимущества, конечное шифрование также сталкивается с вызовами, связанными с законодательством о праве на доступ к данным в различных странах. [4] Некоторые государства стремятся вводить ограничения на использование конечного шифрования из соображений национальной безопасности, что создает сложности для компаний и пользователей, желающих обеспечить конфиденциальность своих данных.

7. Роль конечного шифрования в обеспечении частной жизни [6]

В повседневной жизни конечное шифрование играет важную роль в защите личной информации. Отправляя личные сообщения, фотографии или документы через мессенджеры или электронную почту, люди ожидают, что их данные будут надежно защищены от посторонних глаз. Конечное шифрование обеспечивает эту защиту, создавая прочный барьер для потенциальных нарушителей безопасности.

8. Обзор существующих технологий

На сегодняшний день существует множество технологий, предоставляющих конечное шифрование для различных целей. [7] Мессенджеры, приложения электронной почты, облачные хранилища и другие платформы используют различные методы шифрования для обеспечения безопасности данных своих пользователей. Это свидетельствует о том, что конечное шифрование становится все более распространенным и доступным для широкой аудитории.

9. Будущее конечного шифрования

В будущем конечное шифрование будет продолжать развиваться, стремясь к усовершенствованию методов шифрования и расширению его применения. [8] С постоянным ростом объема цифровых данных и увеличением угроз кибербезопасности, необходимость в надежных методах защиты данных будет только усиливаться, делая конечное шифрование ключевым элементом цифровой безопасности.

Заключение

Конечное шифрование играет важную роль в обеспечении конфиденциальности данных как на уровне индивидуальных пользователей, так и на уровне компаний. Этот метод шифрования обеспечивает защиту от несанкционированного доступа к данным, способствует сохранению доверия пользователей к цифровым сервисам и является неотъемлемым элементом обеспечения частной жизни в цифровом мире. Развитие и распространение конечного шифрования будут иметь важное значение для обеспечения безопасности и конфиденциальности данных в будущем.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика" РИ-2018". – 2018. – С. 149-149.
2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 590-595.
4. Красов А. В. и др. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры.
5. Сахаров Д. В. и др. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети //Научно-аналитический

журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2020. – №. 2. – С. 86-94.
6. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных//Региональная информатика и информационная безопасность. – 2020. – С. 260-262.
7. Волкогонов В. Н. и др. Анализ безопасности wi-fi сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 270-275.
8. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.

References

1. Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks //Regional Informatics"RI-2018". – 2018. – pp. 149-149.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Kazantsev A. A. et al. Creating and managing a Security Operations Center for effective use in real-world environments//Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 590-595.
4. Krasov A.V. et al. Software implementation of intrusion prevention tools and network infrastructure anomalies.
5. Sakharov D. V. et al. Using mathematical forecasting methods to assess the load on the computing power of the IOT network //Scientific and analytical journal "Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia". - 2020. – No. 2. – pp. 86-94.
6. Gelfand A.M. Methods of choosing stegocontainers for data transmission//Regional informatics and information security. – 2020. – pp. 260-262.
7. Volkogonov V. N. et al. Wi-fi network Security Analysis//Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 270-275.
8. Budarny G. S. and others. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.