Перевертун Д.Р. Криптография и её роль в обеспечении информационной безопасности // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 6(32) с. 5–9

Международный журнал информационных технологий и энергоэффективности

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

УДК 004

КРИПТОГРАФИЯ И ЕЁ РОЛЬ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Перевертун Д.Р.
ФГБОУ ВО Санкт-Петербургский государственный университет Телекоммуникаций им. профессора М. А. Бонч-Бруевича, г.Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilaperevertun@gmail.com

Данная статья рассматривает роль криптографии в обеспечении информационной безопасности. Криптография - наука о защите информации путем шифрования и расшифрования данных. Она играет критическую роль в различных сферах, включая коммерцию, финансы, здравоохранение и правительство. Криптография обеспечивает конфиденциальность, целостность и подлинность данных, а также предотвращает несанкционированный доступ и подделку информации. Статья также освещает важные аспекты криптографии, такие как аутентификация, защита от отказа в обслуживании, защита персональных данных и управление ключами. Также упоминается роль криптографии в облачных вычислениях и технологии блокчейн. В заключение, отмечается необходимость постоянного совершенствования криптографических методов в связи с появлением новых угроз и развитием квантовых вычислений.

Ключевые слова: Криптография, информационная безопасность, шифрование, конфиденциальность, аутентификация, защита персональных данных, блокчейн, квантовые вычисления.

CRYPTOGRAPHY AND ITS ROLE IN ENSURING INFORMATION SECURITY

Perevertun D.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: danilaperevertun@gmail.com

This article examines the role of cryptography in ensuring information security. Cryptography is the science of protecting information by encrypting and decrypting data. It plays a critical role in various fields, including commerce, finance, healthcare, and government. Cryptography ensures confidentiality, integrity and authenticity of data, as well as prevents unauthorized access and forgery of information. The article also highlights important aspects of cryptography, such as authentication, denial of service protection, personal data protection and key management. The role of cryptography in cloud computing and blockchain technology is also mentioned. In conclusion, there is a need for continuous improvement of cryptographic methods in connection with the emergence of new threats and the development of quantum computing.

Keywords: Cryptography, information security, encryption, confidentiality, authentication, personal data protection, blockchain, quantum computing.

В современном цифровом мире, где информация играет важнейшую роль, обеспечение ее безопасности является критическим вопросом. Криптография - наука о защите информации путем применения математических алгоритмов и преобразований. Она играет важную роль в обеспечении конфиденциальности, целостности и подлинности данных.

Одной из основных целей криптографии является обеспечение конфиденциальности. Конфиденциальность означает, что только авторизованные пользователи имеют доступ к защищенной информации, и никто другой не может прочитать или понять содержимое. Криптографические алгоритмы используются для шифрования данных, что делает их непонятными для посторонних лиц. Только тот, кто обладает правильным ключом, может расшифровать данные и получить доступ к оригинальной информации. Это особенно важно при передаче конфиденциальных данных, таких как финансовая информация, медицинские записи, персональные данные и коммерческие секреты [1].

Криптография также обеспечивает целостность данных. Целостность гарантирует, что информация остается неизменной и неподделываемой в процессе передачи и хранения. Криптографические хэш-функции используются для создания уникальной сигнатуры для каждого набора данных. Если даже незначительное изменение происходит в данных, это приведет к изменению хэш-значения. Таким образом, при проверке целостности данных можно обнаружить любые несанкционированные изменения.

Помимо конфиденциальности и целостности, криптография обеспечивает подлинность данных. Подлинность гарантирует, что информация и источник информации подлинные и не были подделаны. Криптографические методы цифровой подписи используются для создания электронной подписи, которая является уникальной для каждого отправителя и не может быть подделана. Получатель может проверить электронную подпись, чтобы убедиться в подлинности источника данных и целостности информации.

Криптография играет важную роль в информационной безопасности в различных сферах, включая коммерцию, финансы, здравоохранение, правительство и многое другое. Она позволяет защитить конфиденциальность клиентов и пользователей, предотвратить несанкционированный доступ к чувствительным данным и обеспечить доверие в электронных коммуникациях.

Однако, как и любая другая технология, криптография не является идеальной. С развитием компьютерных мощностей атакующих и появлением новых методов анализа, криптографические алгоритмы могут стать уязвимыми. Поэтому важно постоянно развивать и усовершенствовать криптографические методы и стандарты, чтобы они оставались надежными и устойчивыми к атакам [2].

Кроме основных принципов конфиденциальности, целостности и подлинности, криптография также имеет другие важные аспекты в обеспечении информационной безопасности. Одним из таких аспектов является аутентификация. Аутентификация позволяет проверить подлинность идентификации пользователей или системы. Криптографические методы, такие как цифровые сертификаты и аутентификация на основе открытых ключей (PKI), используются для проверки подлинности идентичности и обеспечения безопасного взаимодействия между участниками.

Криптография также играет роль в обеспечении конфиденциальности при передаче данных по открытым каналам связи, таким как интернет. Протоколы шифрования, такие как SSL/TLS, обеспечивают защищенное соединение между клиентом и сервером, шифруя передаваемую информацию и предотвращая ее перехват и несанкционированный доступ.

Другой важный аспект криптографии - это управление ключами. Криптографические алгоритмы работают на основе ключей, которые используются для шифрования и расшифрования данных. Управление ключами включает в себя безопасное генерирование,

хранение, обмен и уничтожение ключей. Эффективное управление ключами является неотъемлемой частью криптографической системы, поскольку компрометация ключей может привести к нарушению безопасности данных [3-4].

Современные технологии, такие как блокчейн, также полагаются на криптографию для обеспечения безопасности. Блокчейн использует криптографические методы, такие как хэш-функции и цифровые подписи, для обеспечения неподделываемости данных, подтверждения транзакций и создания децентрализованной доверенной среды.

Однако, несмотря на все преимущества криптографии, она не является панацеей и не может полностью исключить угрозы информационной безопасности. Развитие криптоанализа и новых атакующих методов требует постоянного совершенствования криптографических алгоритмов и протоколов. Кроме того, человеческий фактор, такой как ненадлежащая реализация или использование слабых паролей, также может ослабить защиту, даже при использовании сильных криптографических методов.

В целом, криптография играет критическую роль в обеспечении информационной безопасности, обеспечивая конфиденциальность, целостность, подлинность и другие аспекты безопасности данных.

Помимо этого, криптография также является ключевым элементом при обеспечении защиты персональных данных и соблюдении соответствующих законодательных норм и регуляций, таких как Общий регламент по защите данных (GDPR) в Европейском союзе. Криптография позволяет шифровать персональные данные, что делает их непонятными для третьих лиц, и устанавливать контроль над доступом к этим данным. Это особенно важно для организаций, которые собирают, обрабатывают и хранят большие объемы личной информации.

Еще одним важным аспектом криптографии является возможность обеспечить безопасность в облачных вычислениях. Облачные сервисы позволяют организациям хранить и обрабатывать данные удаленно, но одновременно это может повлечь угрозы безопасности. Криптография в облачных вычислениях может быть использована для шифрования данных перед их отправкой в облако, а также для обеспечения конфиденциальности и целостности данных в хранилище облака.

Все более частыми становятся также криптовалюты и технология блокчейн. Криптография является фундаментальным компонентом блокчейна, обеспечивая безопасность транзакций, аутентификацию и защиту от внешних атак. Шифрование используется для создания уникальных цифровых подписей и хэш-функций, которые подтверждают подлинность данных и предотвращают их подделку. Криптография в блокчейне также играет важную роль в обеспечении анонимности и приватности пользователей.

Наконец, следует отметить, что развитие квантовых вычислений представляет новые вызовы и возможности для криптографии. Квантовые компьютеры имеют потенциал взломать некоторые из существующих криптографических алгоритмов, основанных на сложности факторизации и дискретного логарифмирования. В этой связи проводятся исследования по разработке квантовоустойчивых криптографических методов, которые будут способны обеспечить безопасность и в эпоху квантовых вычислений [5-7].

В итоге, криптография играет неотъемлемую роль в обеспечении информационной безопасности, обеспечивая конфиденциальность, целостность, подлинность и другие аспекты

защиты данных. Она применяется в различных областях и технологиях, от сетевой безопасности и защиты персональных данных до облачных вычислений и блокчейна. Однако важно постоянно развивать и совершенствовать криптографические методы, учитывая появление новых угроз и технологических прорывов.

Список литературы

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.
2. Гельфанд А. М. и др. ИНТЕРНЕТ ВЕЩЕЙ (IoT): угрозы безопасности и конфиденциальности //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике //Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
6. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
7. Штеренберг С. И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //ОФТАЛЬМОХИРУРГИЯ. – 2022. – №. 4s. – С. 51-57.

References

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. INTERNET OF THINGS (IoT): SECURITY AND PRIVACY THREATS //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
5. Kosov N. A., Timofeev R. S. Comparison of training methods for convolutional neural networks //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.

6. Kosov N. A., Mazepin P. S., Grishin N. A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57