УДК 004.021

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В СФЕРЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

К.С. Барило, С.Н. Нестеренков, Е.В. Бегляк

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Статья рассматривает криптографические методы защиты информации в сфере электронного документооборота. Основное внимание акцентируется на популярных криптографических методах защиты информации, таких как симметричное и асимметричное шифрование и хэширование в контексте обеспечения безопасности и целостности данных при обмене информацией через открытые каналы, такие как интернет. Описываются способы применения методов криптографической защиты информации для обеспечения конфиденциальности, целостности и доступности электронных документов. Также в данной статье уделяется внимание принципу работы и использованию цифровых подписей для обеспечения целостности данных и защиты авторских прав. В статье будут рассмотрены проблемы и ограничения современной криптографии. Также обсуждаются вызовы и перспективы развития криптографических технологий в сфере электронного документооборота, что делает материал актуальным для специалистов и организаций, работающих с электронными данными.

Ключевые слова: криптография; защита информации; электронный документооборот; безопасность данных; конфиденциальность; целостность; доступность; цифровизация; методы шифрования; доверие к системам.

CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION IN THE FIELD OF ELECTRONIC DOCUMENT MANAGEMENT

K. Barilo, S. Nesterenkov, E. Begliak
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article examines cryptographic methods of information protection in electronic document management, focusing on symmetric and asymmetric encryption and hashing. Their applications for ensuring confidentiality, integrity, and accessibility of documents, as well as the importance of digital signatures, are described. The challenges and prospects for the development of cryptographic technologies in this area are also discussed, which makes the material relevant for specialists and organizations working with electronic data.
Keywords: cryptography, information security, electronic document management, data security, confidentiality, integrity, accessibility, digitalization, encryption methods, trust in systems.

Введение

В современном мире, где цифровизация проникает во все сферы жизни, электронный документооборот становится частью бизнес-процессов и взаимодействия между государственными органами и гражданами. С ростом объемов обрабатываемых данных возникают серьезные угрозы безопасности информации. Криптографические методы защиты являются ключевым инструментом для обеспечения конфиденциальности, целостности и доступности электронных документов.

Криптография, как наука о защищенной передаче и хранении информации, предоставляет мощные средства для защиты данных от несанкционированного доступа и изменений [1]. В данной статье будут рассмотрены основные криптографические методы, используемые для защиты информации в сфере электронного документооборота, а также их влияние на безопасность и эффективность процессов обмена документами.

Основная часть

Основными методами криптографической защиты информации являются:

1. Симметричное шифрование. Симметричное шифрование предполагает использование одного и того же ключа для шифрования и расшифровки данных. Данный метод защиты информации обеспечивает высокую скорость обработки данных и может быть применен для обработки больших объемов информации. Основным ограничением симметричного шифрования является необходимость безопасной передачи ключа между сторонами.

2. Ассиметричное шифрование. Асимметричное шифрование использует пару ключей: открытый и закрытый. Открытый ключ доступен всем участникам передачи данных, а закрытый хранится в секрете. Асимметричное шифрование обеспечивает более высокий уровень безопасности. Данный метод используется для создания цифровых подписей.

3. Хэширование. Хэширование – это процесс преобразования исходных данных в фиксированное значение, называемое хэшем. Хэширование позволяет проверить целостность данных: если изменится хотя бы один бит исходной информации, хэш также изменится. Хэширование широко применяется для хранения паролей и проверки целостности документов.

4. Цифровая подпись. Цифровая подпись используется для аутентификации и подтверждения целостности данных. Данный метод использует ассиметричное

шифрование так, что цифровая подпись создается с помощью закрытого ключа, а проверяется с помощью открытого ключа.

5. Протоколы обмена ключами. Протоколы обмена ключами обеспечивают безопасный обмен криптографическими ключами между сторонами. Примером такого протокола может быть протокол Диффи-Хеллмана [2].

6. Защита на основе атрибутов (Attribute-Based Encryption). Данный способ криптографической защиты информации предполагает шифрование данных с учетом определенных атрибутов, что обеспечивает гибкий доступ к информации.

7. Потоковое шифрование. Данный метод шифрования основан на шифровании данных по одному биту или байту за раз, что позволяет эффективно обрабатывать большие объемы данных. Примерами алгоритмов потокового шифрования являются алгоритмы RC4 и Salsa20 [3].

8. Блочное шифрование. При блочном шифровании данные разделяются на блоки фиксированного размера, после чего каждый блок шифруется отдельно. Примерами алгоритмов блочного шифрования являются алгоритмы AES и Blowfish [3].

9. Комбинированные методы шифрования. Приведенные выше методы могут использоваться в различных комбинациях для обеспечения надежной защиты информации в электронном документообороте.

Шифрование данных предотвращает их перехват и доступ к ним третьих лиц, что особенно важно в условиях передачи данных по открытым каналам связи, таким как интернет.

Хэширование используется для проверки целостности данных, что позволяет обнаружить любые несанкционированные изменения. Данный метод защиты информации активно применяется при хранении пользовательских данных и электронных документов на серверах.

Цифровые подписи, основанные на асимметричном шифровании, позволяют подтвердить авторство и целостность документов [5]. Подтверждение авторства и целостности электронного документа критически важно в юридической и финансовой сферах, где подделка документа может иметь серьезные последствия. Цифровая подпись обеспечивает юридическую значимость электронного документа, что делает его равнозначным бумажному.

Криптографические методы защиты информации также используются для защиты персональных данных в соответствии с законодательными нормами, такими как GDPR. Соблюдение законодательных норм позволяет организациям не только соблюдать правовые требования, но и укреплять доверие клиентов к своим услугам.

Одним из наиболее перспективных направлений развития криптографии является квантовая криптография. Квантовая криптография – направление криптографии, основанное на применении принципов квантовой механики для защиты информации. Квантовая криптография предлагает новые методы защиты, такие как квантовая распределенная ключевая система (QKD) [2]. Квантовая криптография в перспективе способна обеспечить абсолютную безопасность передачи информации.

Несмотря на значительные преимущества криптографических методов защиты информации, существуют сложности реализации безопасности. Примером сложности является обеспечение безопасной передачи ключа для симметричного шифрования по открытым каналам, таким как интернет. Следует учитывать, что с развитием технологий возникают новые угрозы безопасности, требующие постоянного обновления методов защиты.

Перспективы развития криптографических технологий в сфере электронного документооборота связаны с внедрением квантовой криптографии и развитием блокчейн-технологий [5], что обеспечит еще более высокий уровень безопасности.

Заключение

Криптографические методы защиты информации являются основным методом обеспечения безопасности электронного документооборота. Применение криптографии позволяет защитить данные от несанкционированного доступа и изменений, а также повысить доверие к электронным системам. В условиях цифровизации и роста объемов информации необходимость в эффективных методах защиты становится все более актуальной.

Дальнейшее развитие криптографических технологий, таких как квантовая криптография и технологии распределенного реестра, будет способствовать повышению уровня защищенности электронных документов. Исследования в этой области позволят создавать более надежные криптографические алгоритмы, устойчивые к современным угрозам.

Список использованных источников

1. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.
2. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography: Principles and Protocols. Chapman and Hall/CRC.
3. Diffie, W., & Landau, S. (2007). Privacy on the Line: The Politics of Wiretapping and Encryption. MIT Press.
4. Schneier, B. (2015). Secrets and Lies: Digital Security in a Networked World. Wiley.
5. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

References

1. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.
2. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography: Principles and Protocols. Chapman and Hall/CRC.
3. Diffie, W., & Landau, S. (2007). Privacy on the Line: The Politics of Wiretapping and Encryption. MIT Press.
4. Schneier, B. (2015). Secrets and Lies: Digital Security in a Networked World. Wiley.
5. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

Сведения об авторах

Барило К.С., студент кафедры электронных вычислительных машин, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники». kostabarilo12@gmail.com.
Нестеренков С.Н., кандидат технических наук, доцент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники». s.nesterenkov@bsuir.by.
Бегляк Е.В., инженер-программист 1 категории отдела сетевых технологий ЦИИР БГУИР. katarina@bsuir.by.

Information about the authors

Barilo K. student of the Department of Electronic Computing Machines at BSUIR. kostabarilo12@gmail.com.
Nesterenkov S., Candidate of Technical Sciences. Associate Professor. Educational Institution "Belarusian State University of Informatics and Radioelectronics", s.nesterenkov@bsuir.by.
Begliak E., software engineer of the 1st category of the Department of Network Technologies of CIID BSUIR. katarina@bsuir.by.