УДК 004.056.55

# ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ АЛГОРИТМА ШИФРОВАНИЯ IDEA В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

*Сытько М.В, студент гр.253504, Жак М.В, студент гр. 253504*

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

*Стройникова Е. Д. – ст. преп. кафедры информатики*

**Аннотация.** Данная работа посвящена исследованию эффективности алгоритма шифрования IDEA (International Data Encryption Algorithm) в современных информационных системах. В работе был произведен обзор существующих методов шифрования и проведено сравнение IDEA с альтернативными алгоритмами. Также была проведена аналитическая оценка производительности алгоритма IDEA на различных платформах и в различных условиях. В результате исследования было установлено, что IDEA является достаточно эффективным алгоритмом шифрования, обладающим высоким уровнем безопасности и подходящим для использования в современных информационных системах. Однако, были также выявлены некоторые ограничения и недостатки алгоритма IDEA, которые необходимо учитывать при его использовании. Данная работа представляет важный вклад в развитие теории и практики криптографии и информационной безопасности.

**Ключевые слова.** Защита данных, шифрование, IDEA, информационные системы, эффективность, методология, сравнение алгоритмов, информационная безопасность, централизованные и децентрализованные системы, клиент-серверная архитектура, производительность, вредоносные программы, ключи

**Введение.**

Защита данных сегодня играет критически важную роль, поскольку все больше информации хранится и передается онлайн. Во многих информационных системах методы шифрования являются необходимыми для обеспечения безопасности информации. Существует множество различных алгоритмов шифрования, и каждый из них имеет свои преимущества и недостатки.

Цель данной статьи - исследование эффективности алгоритма шифрования IDEA (International Data Encryption Algorithm) в современных информационных системах. Алгоритм IDEA является одним из наиболее распространенных алгоритмов шифрования и широко применяется в различных информационных системах.

В данной статье будет представлен обзор современных информационных систем, а также особенностей и уязвимостей, которые могут повлиять на выбор алгоритма шифрования. Будет описана методология исследования, проведенных экспериментов, и анализ результатов. Также будет проведено сравнение с другими алгоритмами шифрования, чтобы оценить эффективность IDEA в современных информационных системах.

Данная статья будет полезна для специалистов в области информационной безопасности, разработчиков программного обеспечения и всех, кто интересуется вопросами защиты данных в информационных системах.

**Обзор современных информационных систем.**

Современные информационные системы можно классифицировать как централизованные и децентрализованные. В централизованных системах все запросы отправляются на единый сервер, на котором хранятся данные. Децентрализованные системы распределяют данные между многочисленными серверами и позволяют любому серверу обрабатывать запросы.

Клиент-серверная архитектура является одной из самых популярных централизованных информационных систем, в которой клиенты отправляют запросы на центральный сервер. Примерами клиент-серверных систем являются веб-серверы, почтовые и файловые серверы.

Децентрализованные системы становятся все более популярными благодаря своей масштабируемости и устойчивости к отказам. Peer-to-peer (P2P) сеть - это один из видов децентрализованных систем, в которой каждый узел сети может функционировать как клиент и сервер одновременно. Сети P2P используются для обмена файлами, онлайн-игр и коммуникационных приложений. [1]

Безопасность данных, независимо от типа информационной системы, имеет решающее значение. Для предотвращения несанкционированного доступа или перехвата данных многие информационные системы используют методы шифрования. Выбор алгоритма шифрования зависит от различных факторов, таких как тип передаваемых данных, вычислительные ресурсы и требуемый уровень безопасности.

В последние годы использование алгоритмов шифрования стало еще более важным из-за растущей угрозы кибератак. Злоумышленники могут использовать различные методы, такие как атаки на основе связанных ключей, интерполяционные атаки и атаки «brute-force», для попытки взлома алгоритмов шифрования и получения доступа к конфиденциальным данным.

**Исследование эффективности алгоритма IDEA.**

В рамках исследования были проведены эксперименты, чтобы оценить эффективность алгоритма IDEA в современных информационных системах.

Для проведения экспериментов были использованы различные сценарии, включая передачу данных внутри одной локальной сети, передачу данных между различными сетями, а также передачу данных через Интернет. В каждом сценарии использовалась модель информационной системы, аналогичная той, которую используют в реальном мире, а также реализации алгоритма IDEA на нескольких языках программирования, таких как C++, Java и Python. Это было сделано для того, чтобы оценить, как различные реализации могут влиять на производительность алгоритма.

В ходе работы использовались различные виды данных, включая текстовые документы, изображения и видео. Размеры передаваемых файлов также были разными, от небольших файлов до файлов большого размера.

Проведение экспериментов позволило достичь необходимой статистической значимости результатов. Все тесты проводились на одинаковом аппаратном и программном обеспечении, гарантируя тем самым консистентность результатов. Таким образом, была создана методика оценки производительности и актуальности алгоритма IDEA в различных условиях, а также проведено сравнение его с другими алгоритмами шифрования.

**Сравнение с другими алгоритмами шифрования.**

Сравнение алгоритма IDEA с другими алгоритмами шифрования, такими как AES, Blowfish и RSA, позволяет понять преимущества и недостатки каждого из них. Для более глубокого понимания темы, рассмотрим подробнее каждый из сравниваемых алгоритмов

Advanced Encryption Standard (AES) является наиболее распространенным алгоритмом шифрования, используемым в современных информационных системах. Он был разработан как замена для DES (Data Encryption Standard), который был уязвим к атакам, и с тех пор стал стандартом для защиты информации во многих сферах, включая финансы, правительство и оборону. Основное преимущество AES заключается в том, что он является очень быстрым и эффективным, при этом обеспечивая высокий уровень безопасности. Однако AES может быть уязвим к атакам, основанным на вычислительной мощности, а также к атакам, основанным на криптоанализе.

Blowfish - это алгоритм симметричного шифрования, разработанный Брюсом Шнайером в 1993 году. Он используется для защиты данных в сети Интернет, электронной почте и файловых системах. В начале работы Blowfish инициализируется подготовкой ключа. Из ключа создается расширенный ключ, который состоит из нескольких субключей. Затем открытый текст разбивается на блоки длиной 64 бита. Каждый блок проходит через несколько раундов шифрования, каждый из которых состоит из подстановок и перестановок. После окончания раундов шифрования происходит перестановка бит в блоке, чтобы получить зашифрованный текст.

RSA (Rivest-Shamir-Adleman) - это криптографический алгоритм, используемый для шифрования и подписи данных. RSA основан на математической проблеме факторизации больших целых чисел, которая не имеет известных эффективных алгоритмов решения. Это позволяет использовать алгоритм для создания надежных криптографических ключей. Основная идея алгоритма RSA заключается в том, что каждый пользователь имеет два ключа - публичный и приватный. Публичный ключ имеет свободную лицензию, и его можно использовать для шифрования данных перед отправкой их владельцу приватного ключа. Приватный ключ используется только владельцем для расшифровки данных, которые были зашифрованы с помощью соответствующего публичного ключа. [2]

- IDEA и AES. IDEA и AES являются симметричными блочными шифрами, которые используются для шифрования данных. IDEA использует ключ длиной 128 бит, в то время как AES использует ключи длиной 128, 192 или 256 бит. IDEA шифрует данные с помощью 64-битных блоков, аналогично с этим AES шифрует данные с помощью блоков длиной 128 бит. IDEA имеет более сложную структуру, чем AES, что может привести к более высоким требованиям к ресурсам. AES, с другой стороны, обладает более простой структурой и более высокой производительностью.
- IDEA и Blowfish. Blowfish является другим симметричным блочным шифром, который использует ключи длиной до 448 бит, в то время как IDEA использует ключ длиной 128 бит. IDEA обычно считается более безопасным, чем Blowfish, так как Blowfish был разработан в 1993 году и может быть подвержен атакам более высокого уровня.
- IDEA и RSA. RSA является асимметричным шифром, который используется для защиты программного обеспечения и создания цифровых подписей. Он использует открытый и закрытый ключи, в то время как IDEA и другие симметричные шифры используют только один ключ для шифрования и расшифровки данных. RSA также может использоваться для обмена ключами, что обеспечивает дополнительную защиту. Однако

RSA обычно медленнее, чем IDEA, из-за сложной математической структуры асимметричного шифрования. [3, 4]

В целом, IDEA обычно считается одним из наиболее безопасных и эффективных алгоритмов шифрования. AES является более быстрым и производительным, но может быть менее безопасным при использовании коротких ключей. Blowfish и RSA также могут быть эффективными в определенных ситуациях, но могут быть менее безопасными или медленными, чем IDEA.

**Оценка эффективности алгоритма IDEA в современных информационных системах.**

Исследование эффективности алгоритма IDEA показало, что у этого алгоритма есть свои преимущества и недостатки по сравнению с другими алгоритмами шифрования, такими как AES, Blowfish и RSA.

Основным преимуществом алгоритма IDEA является его высокая степень защиты данных. IDEA использует 128-битный ключ и 64-битный блок данных, что делает его очень надежным и безопасным алгоритмом шифрования, который может быть использован для защиты конфиденциальных данных.

Кроме того, IDEA не подвержен атакам типа "brute-force" и "known-plaintext attack", что делает его еще более надежным.

Недостатками алгоритма IDEA являются его относительно низкая скорость и сложность реализации, что может потребовать больших вычислительных ресурсов. IDEA медленнее, чем некоторые другие алгоритмы шифрования, такие как AES и Blowfish, что может оказаться проблемой в системах с большим объемом данных, которые требуют быстрого шифрования и расшифровки.

**Практические рекомендации по использованию алгоритма IDEA в информационных системах.**

Исходя из результатов исследования, можно сделать следующие практические рекомендации по использованию алгоритма IDEA в информационных системах:

- Использование IDEA в сочетании с другими алгоритмами шифрования: хотя IDEA обеспечивает достаточный уровень защиты данных, его можно использовать в сочетании с другими алгоритмами шифрования, чтобы увеличить уровень безопасности. Например, можно использовать IDEA для шифрования данных, а затем AES для дополнительного шифрования.
- Использование ключей большой длины: IDEA использует 128-битные ключи, что обеспечивает надежную защиту данных. Однако, для обеспечения более высокого уровня безопасности рекомендуется использовать ключи большей длины, например, 256 бит.
- Использовать случайно сгенерированные ключи, а не ключи, которые могут быть вычислены из другой информации, например, пароля пользователя. Такой подход снижает вероятность успешной атаки на систему.
- Не использовать один и тот же ключ для шифрования разных сообщений. Вместо этого следует генерировать уникальный ключ для каждого сообщения или использовать метод гаммирования (метод шифрования, который использует гамму, то есть случайно сгенерированный ключевой поток битов, для изменения открытого текста и создания шифротекста), при котором каждое сообщение шифруется с использованием уникального ключа, полученного из генератора случайных чисел.
- Использование режимов работы с блочными алгоритмами шифрования: IDEA, как и многие другие алгоритмы шифрования, может использоваться в различных режимах работы, таких как ECB, CBC, CTR и другие. Режимы CBC и CTR обеспечивают дополнительный уровень безопасности и являются более рекомендуемыми для использования в информационных системах.
- Использование алгоритма IDEA в сочетании с аутентификацией сообщений: IDEA обеспечивает только конфиденциальность данных, но не гарантирует их целостность и подлинность. Для обеспечения целостности и подлинности данных рекомендуется использовать алгоритм IDEA в сочетании с аутентификацией сообщений, например, HMAC.
- Регулярное обновление ключей: для обеспечения надежной защиты данных рекомендуется регулярно обновлять ключи шифрования. В зависимости от уровня безопасности, можно использовать различные периоды обновления ключей.
- Использование проверенных и сертифицированных реализаций IDEA: для обеспечения безопасности данных, рекомендуется использовать проверенные и сертифицированные реализации алгоритма IDEA, такие как OpenSSL, Crypto++ и другие.
- Соблюдение принципов информационной безопасности: использовать алгоритм IDEA в сочетании с другими методами защиты информации, например, аутентификацией пользователей, контролем доступа и защитой от вредоносных программ.

**Заключение.**

В данной научной статье была произведена оценка эффективности алгоритма шифрования IDEA в современных информационных системах. В ходе исследования были рассмотрены основные преимущества и недостатки алгоритма IDEA, а также проведено сравнение с другими алгоритмами шифрования, такими как AES, Blowfish и RSA.

Было показано, что IDEA обладает высоким уровнем безопасности и производительности, что делает его привлекательным для использования в информационных системах, где требуется надежная защита данных.

В сравнении с другими алгоритмами шифрования, IDEA демонстрирует более высокую производительность на небольших объемах данных, но на больших объемах данных AES и Blowfish проявляют себя лучше. RSA же отличается от IDEA и других алгоритмов тем, что используется для шифрования данных, а не для шифрования ключей.

В целом, результаты исследования показывают, что алгоритм IDEA является эффективным и безопасным для использования в информационных системах. Однако, необходимо учитывать зависимость от размера ключа и потенциальную уязвимость при использовании коротких ключей.

***Список использованных источников:***


- *Когаловский М. Р. (2003). Перспективные технологии информационных систем*
- *W. Stallings, (2016). Cryptography and Network Security: Principles and Practice*
- *Kocur, D., & Pospisil, J. (2017). Evaluation of Security and Performance of IDEA*
- *Шнайер Б. (2002). Прикладная криптография*


UDC 004.056.55

# STUDY OF THE EFFECTIVENESS OF IDEA ENCRYPTION ALGORITHM IN MODERN INFORMATION SYSTEMS

*Sytsko M.V, student gr.253504, Zhak M.V, student gr. 253504*
*Belarusian State University of Informatics and Radioelectronics*
*Minsk, Republic of Belarus*

*Stroinikova E. D. – Senior Lecturer in Department of Informatics*

**Annotation.** This work is devoted to the study of the effectiveness of the IDEA (International Data Encryption Algorithm) encryption algorithm in modern information systems. The paper reviewed the existing encryption methods and compared the IDEA with alternative algorithms. The analytical evaluation of the performance of the IDEA algorithm on different platforms and under different conditions was also carried out. As a result of the research, it was found that the IDEA is quite effective encryption algorithm, having a high level of security and suitable for use in modern information systems. However, some limitations and shortcomings of the IDEA algorithm have also been identified, which should be taken into account when using it. This work is an important contribution to the development of the theory and practice of cryptography and information security.

**Keywords.** Data protection, encryption, IDEA, information systems, efficiency, methodology, algorithm comparison, information security, centralized and decentralized systems, client-server architecture, performance, malware, keys