4. Анализ отрасли при создании конкурентной стратегии – «5 сил Портера» [Электронный ресурс]. – Режим доступа: https://artsdelka.ru/pyat-sil-portera/. – Дата доступа: 09.10.2024.

УДК 004.4

А.О. Фенин, Н.А. Горбунова
Карагандинский университет им. Е.А. Букетова
Караганда, Казахстан

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Аннотация. *Статья посвящена анализу современных алгоритмов шифрования данных. Дан обзор наиболее распространенных алгоритмов шифрования. Представлен анализ уязвимостей современных алгоритмов шифрования. В заключении делаются выводы о том, что необходимо использовать комплексные методы защиты данных и периодически обновлять используемые алгоритмы шифрования.*

A.O. Fenin, N.A. Gorbunova
Karaganda Buketov University
Karaganda, Kazakhstan

COMPARATIVE ANALYSIS OF MODERN ENCRYPTION ALGORITHMS

Abstract. *The article is devoted to the analysis of modern data encryption algorithms. An overview of the most common encryption algorithms is given. An analysis of the vulnerabilities of modern encryption algorithms is presented. In conclusion, it is concluded that it is necessary to use complex data protection methods and periodically update encryption methods.*

В связи с увеличившимся в современных условиях объемом передаваемой, получаемой и хранимой информации, как никогда актуальна проблема защиты данных. Для противодействия этому применяют разнообразные способы защиты информации, реализованные посредством внедрения специализированного ПО и комплексных систем защиты.

В литературе предлагается следующая классификация средств защиты информации: средства защиты от несанкционированного доступа; системы анализа и моделирования информационных потоков (case-системы); системы мониторинга сетей; анализаторы

протоколов; антивирусные средства; межсетевые экраны; криптографические средства; системы резервного копирования; системы бесперебойного питания; системы аутентификации; средства предотвращения взлома корпусов и краж оборудования; средства контроля доступа в помещения; инструментальные средства анализа систем защиты.

Рассмотрим современные криптографические методы защиты. Как известно, криптография – наука о шифрах – первоначально изучала методы шифрования информации, т.е. обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст. Традиционная криптография образует раздел симметричных криптосистем, в которых зашифровывание и расшифровывание проводится с использованием одного и того же секретного ключа. В наши дни криптография используется для обеспечения безопасности информации как на государственном уровне так и для организаций и частных лиц.

В большинстве случаев данные приходится защищать от несанкционированного доступа. Например, в прошлом году в результате утечки данных было раскрыто более 4,1 миллиарда записей. В одной из последних утечек китайские хакеры выудили более 60 000 электронных писем у сотрудников Государственного департамента.

Подобные инциденты свидетельствуют о том, что алгоритмы шифрования и управление ключами шифрования являются важнейшим условием безопасного общения в сети.

В настоящее время используется два типа шифрования: симметричное и асимметричное шифрование – два разных криптографических метода, каждый из которых имеет свои сильные и слабые стороны, а также варианты использования. В симметричном шифровании используется один ключ для шифрования и дешифрования, в то время как в асимметричном шифровании используется пара ключей – открытый ключ для шифрования информации и закрытый ключ для дешифрования данных.

Симметричное шифрование идеально подходит для защиты больших объемов данных, локального хранения файлов, шифрования баз данных и частных сетевых коммуникаций. Асимметричное шифрование жизненно необходимо для защиты интернет-коммуникаций, конфиденциальности электронной почты и обеспечения возможности использования цифровых подписей для аутентификации.

На практике системы используют комбинацию симметричного и асимметричного шифрования. Например, при асимметричном шифровании можно безопасно обмениваться ключом симметричного шифрования, который затем используется для массовой передачи данных с помощью симметричного шифрования.

Этот гибридный подход сочетает в себе эффективность симметричного шифрования с возможностями обмена ключами асимметричного шифрования, обеспечивая безопасное и практичное решение для различных сценариев.

Криптография с симметричным ключом используется в электронных банковских операциях. Когда клиент запускает транзакцию, банк шифрует данные о ней с помощью общего симметричного ключа, известного банку и клиенту.

Затем клиент может расшифровать информацию, используя тот же ключ, чтобы подтвердить подлинность транзакции. Чтобы соответствовать нормативным требованиям, организации часто используют симметричное шифрование для защиты конфиденциальных данных в своих базах данных.

Например, безопасность веб-сайтов часто полагается на асимметричное шифрование для безопасных HTTPS-соединений, чтобы защитить обмен данными между пользователями и веб-сайтами.

Безопасное общение по электронной почте – еще один реальный пример асимметричного шифрования в действии. Этот метод гарантирует сохранение конфиденциальности конфиденциальной информации во время передачи электронной почты.

Таким образом, алгоритм шифрования – это набор математических правил и процессов, используемых для преобразования открытого текста (незашифрованных данных) в шифрованный текст (зашифрованные данные), что затрудняет неавторизованным лицам доступ к исходной информации или ее понимание без соответствующего ключа для расшифровки.

Различные алгоритмы шифрования могут быть более подходящими для определенных типов данных или приложений, исходя из требований к безопасности, скорости и ресурсам. Например, алгоритмы с симметричными ключами работают быстро, но менее безопасны для передачи данных. Асимметричные ключевые алгоритмы лучше подходят для шифрования данных в пути, но работают медленнее.

Наконец, хэш-функции создают из данных хэш-коды

фиксированной длины. Они подходят для проверки целостности данных.

С годами методы шифрования эволюционировали от простых подстановочных шифров, таких как шифры Цезаря, до современных криптографических алгоритмов, таких как DES, AES, RSA и ECC.

Существует два основных метода симметричного шифрования: блочные шифры и потоковые шифры.

Блочный шифр делит данные на блоки фиксированного размера для шифрования, что делает его подходящим для структурированных данных, таких как файлы. Они предсказуемы, но могут иметь уязвимые места при неправильном использовании. AES – это хорошо известный блочный шифр.

Сегодня симметричный алгоритм AES защищает различные приложения и системы, от защиты передачи конфиденциальных данных через Интернет до шифрования секретной информации в хранилищах. Сочетание безопасности и эффективности сделало его краеугольным камнем современных методов шифрования, обеспечивающих конфиденциальность и целостность данных – от транзакций электронной коммерции до безопасной передачи конфиденциальных данных.

Наиболее распространенные методы асимметричного шифрования: RSA, ECC, Диффи-Хеллмана.

Rivest Shamir Adleman (RSA) – это алгоритм асимметричного шифрования, созданный Роном Ривестом, Ади Шамиром и Леонардом Адлеманом в 1977 году. Он является неотъемлемой частью протоколов SSL/TLS, обеспечивающих безопасную передачу данных в Интернете.

RSA превосходит всех в области безопасного шифрования данных и цифровых подписей. Он широко распространен и совместим. Тем не менее, он требует периодического увеличения размера ключа в связи с ростом вычислительной мощности, а управление ключами имеет решающее значение для безопасности.

Безопасность RSA основана на сложности факторизации больших чисел, и будущие квантовые компьютеры могут представлять угрозу. Неадекватное управление ключами также может привести к нарушениям.

Криптография эллиптических кривых (ECC) – это асимметричный метод шифрования, который отличается от других методов шифрования данных тем, что не полагается на проблемы больших чисел. Вместо этого она использует математику кривых.

Основные случаи использования Диффи-Хеллмана включают

создание защищенных каналов в зашифрованных коммуникациях, таких как SSL/TLS, которые обеспечивают безопасность передачи данных в Интернете. VPN и приложения для обмена сообщениями также используют его. Стратегии защиты включают цифровые сертификаты и такие протоколы, как Internet Key Exchange (IKE) для аутентификации. Длинные простые числа также укрепляют безопасность.

Алгоритм цифровой подписи (DSA) создает цифровые подписи (известные как цифровые печати) с помощью закрытых ключей для обеспечения подлинности сообщений. Получатели используют открытые ключи для проверки этих подписей, гарантируя целостность сообщения и его источник. В отличие от шифрования RSA, которое сосредоточено на конфиденциальности, DSA концентрируется на целостности и подлинности данных.

DSA обеспечивает безопасность обмена электронной почтой, обновлений программного обеспечения и цифровых подписей в правительственных, финансовых и ориентированных на безопасность приложениях. Его опасения включают риск компрометации закрытого ключа и потенциальные проблемы с эффективностью.

Выбор алгоритма шифрования является основополагающим фактором безопасности данных, а постоянное знакомство с новейшими методами шифрования данных имеет решающее значение для сохранения цифровой конфиденциальности.

Таким образом, защита данных с помощью таких алгоритмов шифрования, как AES, RSA и DES, обеспечивает наиболее надежную и эффективную защиту. Более того, есть возможность комбинировать различные методы шифрования данных, чтобы добиться еще более высоких результатов.

Список использованных источников

1. Ященко В. В. Введение в криптографию. СПб.: Питер, 2001.

2. Бабаш А. В. Криптографические методы защиты информации: учебник для вузов / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2016.

3. Ахмедова Х. Х. Тенденции развития и проблемы современной криптографии. «Scientific Progress Vol. 1 Issue 3.»

4. Бабаш А. В. Актуальные проблемы криптографии. – Материалы XVI Всероссийской научно-практической конференции.

5. Mohammed Nazeh Abdul Wahid, Abdulrahman Ali, Babak Esparham and Mohamed Marwan. A Comparison of Cryptographic

Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention - Journal of Computer Science Applications and Information Technology

УДК 004.8

М.Чарыева
Институт телекоммуникаций и информатики
Ашхабад Туркменистан

ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ОБРАЗОВАНИЕ: АДАПТИВНОЕ ОБУЧЕНИЕ, ПЕРСОНАЛИЗАЦИЯ И ВЫЗОВЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Аннотация. *Внедрение ИИ в образовательные системы позволяет разрабатывать адаптивные учебные платформы, интеллектуальных ассистентов и системы для анализа успеваемости, что делает процесс обучения более гибким и эффективным. В статье рассматриваются ключевые преимущества использования ИИ в образовании, включая возможность адаптации обучения к индивидуальным потребностям учащихся, автоматизацию рутинных задач для преподавателей и анализ данных для прогнозирования учебных результатов. Также обсуждаются вызовы внедрения ИИ в образовательные системы, такие как вопросы этики, конфиденциальности данных и необходимость подготовки педагогов к работе с новыми технологиями. Рассмотрение этих аспектов позволяет оценить потенциал и риски ИИ для образовательной сферы.*

M.Charyeva
Institute of Telecommunications and Informatics
Ashgabat Turkmenistan

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON EDUCATION: ADAPTIVE LEARNING, PERSONALIZATION AND CHALLENGES OF DIGITAL TRANSFORMATION

Abstract*. The introduction of AI into educational systems allows the development of adaptive learning platforms, intelligent assistants and systems for analyzing academic performance, which makes the learning process more flexible and efficient. The article discusses the key advantages of using AI in education, including the ability to adapt learning to the individual needs of students, automation of routine tasks for teachers and data analysis to predict learning outcomes. The challenges of introducing AI into educational systems, such as ethics, data privacy, and the need to prepare teachers to work with new technologies, are also discussed. Consideration of these aspects makes it*