УДК: 004.056.5
ББК: 16.84
ГРНТИ: 81.93.29

Пелешенко Татьяна Александровна, *доцент кафедры вычислительной математики и кибернетики факультета математики и компьютерных наук имени профессора Н. И. Червякова, ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, Россия.*

Peleshenko Tatiana A., *Associate Professor, Department of Computational Mathematics and Cybernetics, Faculty of Mathematics and Computer Sciences named after Prof. Nikolay Chervyakov, North Caucasus Federal University, Stavropol, Russia.*

Чернышев Савва Андреевич, Чубенко Анастасия Денисовна, *обучающиеся, МБОУ «Средняя общеобразовательная школа № 28», Ставрополь, Россия.*

Chernyshev Savva A., Chubenko Anastasia D., *Students, School No. 28, Stavropol, Russia.*

Гиш Александр Сергеевич, *студент кафедры вычислительной математики и кибернетики факультета математики и компьютерных наук имени профессора Н. И. Червякова, ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, Россия.*

Gish Alexander S., *Student, Department of Computational Mathematics and Cybernetics, Faculty of Mathematics and Computer Sciences named after Prof. Nikolay Chervyakov, North Caucasus Federal University, Stavropol, Russia.*

Филатов Николай Александрович, *студент кафедры КБ-14 «Цифровые технологии обработки данных» Института кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет», Москва, Россия.*

Filatov Nikolay A., *Student, Department KB-14 "Digital data processing technologies", Institute for Cybersecurity and Digital Technologies, MIREA – Russian Technological University, Moscow, Russia.*

Исследование применения в обучении криптографических алгоритмов в цифровую эпоху: проблемы и перспективы

Аннотация. *Данная работа направлена на рассмотрение методов внедрения основ криптографии в образовательный процесс. Для начала обучения студентов и школьников основам защиты информации авторы предлагают воспользоваться базовыми криптографическими алгоритмами, такими как: шифр Цезаря, шифр Виженера. Рассмотрены основные направления современной криптографии, проанализированы типы алгоритмов шифрования и их особенности. Представлены результаты опроса, направленного на выявление уровня осведомлённости о криптографии, её важности и интереса к её изучению.*

Ключевые слова: *криптография, шифрование, социальные сети, мессенджеры, облачные хранилища, компьютеры, нейросеть, платёжная информация, утечки.*

Research on the Use of Cryptographic Algorithms in the Digital Age: Problems and Prospects

Abstract. *This work is aimed at considering the methods of introducing the basics of cryptography into the educational process. To begin teaching students and schoolchildren the basics of information security, the authors suggest using basic cryptographic algorithms, such as the Caesar cipher, the Vigenere cipher. The main trends in modern cryptography are examined, and the types of encryption algorithms and their characteristics are analyzed. The results of a survey aimed at identifying the level of awareness of cryptography, its importance, and interest in its study are presented.*

Keywords: *cryptography, encryption, social networks, instant messengers, cloud storages, computers, neural network, payment information, leaks.*

Актуальность

В современном мире шифрование играет ключевую роль в обеспечении безопасности и конфиденциальности данных пользователей. Криптография помогает защитить личную информацию (номера банковских карт, сообщения в социальных сетях и т. д.) от несанкционированного доступа. Данный вид защиты используется во многих отраслях жизни, таких как интернет-банкинг, онлайн-платежи, защита электронных почт, мессенджеров, облачных хранилищ, Wi-Fi сетей, цифровых подписей и электронных документов. В современном мире смартфоны и компьютеры шифруют данные пользователей на уровне диска, а в умных устройствах, таких как камеры наблюдения, шифрование используется для повышения защиты самого устройства. В государственных и частных компаниях криптографию используют для предотвращения утечек секретных данных. Таким образом, криптография является незаменимой технологией, обеспечивающей защиту конфиденциальной информации в различных областях жизни.

Криптография, как наука о защите информации, прошла долгий путь от примитивных методов древности до сложных алгоритмов, лежащих в основе современных цифровых систем. Её история тесно связана с потребностью человечества в сохранении тайн – от военных донесений до личной переписки. Одним из первых известных примеров является шифр Цезаря, использовавшийся в Древнем Риме. Принцип его работы прост: каждая буква в сообщении заменялась на другую, смещённую в алфавите на фиксированное число позиций. Например, при сдвиге на 3 буква «А» превращалась в «Г». Несмотря на уязвимость к частотному анализу этот метод заложил основу для более сложных алгоритмов подстановки и перестановки.

В Средневековье криптография усложнилась. Например, шифр Виженера ввёл использование ключевого слова, что значительно повысило устойчивость к взлому. Однако настоящий прорыв произошёл в XX веке с появлением компьютеров. Механические устройства, такие как немецкая Enigma, использовавшаяся во Второй мировой

войне, продемонстрировали, как инженерные решения могут сочетаться с криптографией. Взлом этого шифра британскими учёными, включая Алана Тьюринга, стал поворотным моментом в истории криптоанализа.

Современная криптография делится на два основных направления: симметричное и асимметричное шифрование. В симметричных системах, таких как AES (Advanced Encryption Standard), для шифрования и дешифрования используется один ключ. AES, принятый в 2001 году, стал стандартом благодаря своей скорости и надёжности. Он применяется в банковских транзакциях, защите Wi-Fi сетей (WPA2/WPA3) и шифровании файлов на жёстких дисках. Предшественник AES – алгоритм DES (Data Encryption Standard) – устарел из-за малой длины ключа (56 бит), но сыграл важную роль в развитии криптографии.

Асимметричная криптография решает проблему безопасного обмена ключами. Здесь используются два ключа: открытый (для шифрования) и закрытый (для дешифрования). Яркий пример – алгоритм RSA, основанный на сложности разложения больших чисел на множители. RSA применяется в цифровых подписях и протоколе HTTPS для установки защищённого соединения. Другой популярный метод – ECC (Elliptic Curve Cryptography), который обеспечивает аналогичную безопасность при меньшей длине ключа, что особенно важно для мобильных устройств. Типы алгоритмов шифрования и их особенности представлены в табл. 1.

Таблица 1

Применение	Тип алгоритма шифрования	Уровень защищённости	Возможные риски
Электронная почта	SSL/TLS	Высокий	Атаки посредника (MITM), утечка ключей
Онлайн-банкинг	RSA, AES	Высокий	Фишинговые атаки, уязвимости браузера
Социальные сети	HTTPS, TLS	Средний	Взлом аккаунтов, кража данных пользователей
Мессенджеры	End-to-end encryption	Высокий	Уязвимости серверной части приложения
Смартфоны	Биометрическая аутентификация, шифрование диска	Высокий	Физический доступ к устройству, ошибки в ПО
Интернет-магазины	SSL/TLS, PCI DSS	Высокий	Утечка платёжных данных, фишинг

Для оценки эффективности интеграции криптографии в учебные программы было проведено небольшое исследование среди студентов старших курсов технических специальностей. В рамках исследования студентам было предложено пройти

курс, включающий как теоретические основы криптографии, так и практические задания. В начале курса только 30 % студентов могли объяснить, как работает шифр Цезаря, и лишь 15 % имели представление о современных алгоритмах, таких как AES и RSA. После завершения курса результаты значительно улучшились: 85 % студентов смогли самостоятельно реализовать шифр Цезаря и объяснить его принцип работы, а 70 % продемонстрировали понимание работы AES и RSA. Кроме того, 90 % студентов отметили, что курс помог им лучше понять, как обеспечивается безопасность данных в повседневной жизни, и выразили интерес к дальнейшему изучению криптографии.

Для более детального анализа отношения студентов к криптографии был проведён опрос, в котором приняли участие 50 студентов. Вопросы были направлены на выявление уровня осведомлённости о криптографии, её важности и интереса к её изучению.

Насколько вы знакомы с понятием криптографии?

- 60 % студентов ответили, что имеют базовое представление.
- 25 % отметили, что знают о криптографии только из фильмов или новостей.
- 15 % заявили, что никогда не слышали о криптографии до начала курса.

Считаете ли вы, что криптография важна в современном мире?

- 95 % студентов ответили, что криптография крайне важна для защиты данных.
- 5 % затруднились с ответом.

Хотели бы вы углублённо изучать криптографию в рамках учебной программы?

- 80 % студентов выразили желание изучать криптографию более детально.
- 15 % ответили, что им достаточно базовых знаний.
- 5 % не заинтересованы в дальнейшем изучении.

Как вы оцениваете практическую пользу криптографии в повседневной жизни?

- 70 % студентов отметили, что криптография полезна для защиты личных данных.
- 20 % считают, что её применение ограничено профессиональной сферой.
- 10 % затруднились с ответом.

Результаты опроса подтверждают, что студенты осознают важность криптографии, но многие из них до начала курса не имели достаточных знаний в этой области. После прохождения курса интерес к криптографии значительно возрос, что свидетельствует о необходимости её интеграции в учебные программы [3; 9]. Интеграция криптографии в учебные программы – это важный шаг в подготовке студентов к вызовам цифровой эпохи.

Список литературы

1. *Дубровин С. И.*, *Белянкин Н. Я.* Искусственный интеллект и криптография. Обзор и перспективы // Аллея науки. 2024. Т. 1, № 11. С. 669–672.

2. *Зуфарова А. С.*, *Бузыкова Ю. С.*, *Бурыкина А. Д.* Актуальность внедрения основ криптографии в школьную программу: анализ целей, возможные подходы и средства программной поддержки // Управление образованием: теория и практика. 2023. Т. 13, № 5. С. 201–212.

3. *Кузнецова В. Ю.* Обеспечение компетентности российских школьников в вопросах криптографии: анализ целей, возможных подходов и технологий, средств их программной поддержки // Прикаспийский журнал: управление и высокие технологии. 2019. № 2 (46). С.163–170.

4. *Осипова А. А.* Криптография как средство развития аналитического мышления младших школьников // Современная начальная школа. 2023. № 8 (51). С. 47–49.

5. *Перекатова А. Д.*, *Горшкова Т. В.* Таинственные страницы истории: криптография вчера и сегодня // Вестник науки. 2019. Т. 1, № 7. С. 37–50.

References

1. Dubrovin S. I., Belyankin N. Ya. Iskusstvennyy intellekt i kriptografiya. Obzor i perspektivy. *Alleya nauki*. 2024, Vol. 1, No. 11, pp. 669–672.

2. Zufarova A. S., Buzykova Yu. S., Burykina A. D. Aktualnost vnedreniya osnov kriptografii v shkolnuyu programmu: analiz tseley, vozmozhnye podkhody i sredstva programmnoy podderzhki. *Upravlenie obrazovaniem: teoriya i praktika*. 2023, Vol. 13, No. 5, pp. 201–212.

3. Kuznetsova V. Yu. Obespechenie kompetentnosti rossiyskikh shkolnikov v voprosakh kriptografii: analiz tseley, vozmozhnykh podkhodov i tekhnologiy, sredstv ikh programmnoy podderzhki. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii*. 2019, No. 2 (46), pp.163–170.

4. Osipova A. A. Kriptografiya kak sredstvo razvitiya analiticheskogo myshleniya mladshikh shkolnikov. *Sovremennaya nachalnaya shkola*. 2023, No. 8 (51), pp. 47–49.

5. Perekatova A. D., Gorshkova T. V. Tainstvennye stranitsy istorii: kriptografiya vchera i segodnya. *Vestnik nauki*. 2019, Vol. 1, No. 7, pp. 37–50.