ЦИФРОВЫЕ ТЕХНОЛОГИИ | DIGITAL TECHNOLOGIES

Система безопасного обмена данными Send.1hut.ru: применение AES-256-CBC в академической среде востоковедения

Send.1hut.ru Secure Data Exchange System: Applying AES-256-CBC to Oriental Studies

Спиридонов Егор Афанасьевич

Институт востоковедения Российской академии наук, Лаборатория цифровых исследований современного Востока ИВ РАН, ведущий специалист

e.spiridonov@ivran.ru

Spiridonov Egor Afanasyevich

Institute of Oriental Studies of Russian Academy of Sciences, Digital Research Laboratory of Contemporary East, Leading specialist

ORCID: 0009-0004-6933-6407

В статье рассматривается отечественная система безопасного обмена информацией Send.1hut.ru, разработанная Лабораторией цифровых исследований современного Востока Института востоковедения РАН. Сервис реализует алгоритм AES-256-CBC, обеспечивая высокий уровень защиты исследовательских и архивных данных. Представлены принципы работы алгоритма, структура сервиса, механизмы защиты и примеры применения в академической практике востоковедов. Анализируются существующие угрозы кибербезопасности, включая фишинг, взломы мессенджеров и утечки данных через электронную почту. Отмечается значение сервиса для формирования культуры безопасного обмена информацией в научной среде.

Ключевые слова: кибербезопасность, передача данных, AES-256, защита данных исследований

This article examines the Russian secure information exchange system Send.1hut.ru, developed by the Laboratory of Digital Studies of the Modern East at the Institute of Oriental Studies of the Russian Academy of Sciences. The service implements the AES-256-CBC algorithm, providing a high level of protection for research and archival data. It presents the algorithm's operating principles, the service's structure, security mechanisms, and examples of its application in the academic practice of Asian studies. It analyzes existing cybersecurity threats, including phishing, messaging app hacks, and email data leaks. The service's importance for fostering a culture of secure information exchange in the scientific community is highlighted.

Keywords: Cybersecurity, data transmission, AES-256, research data protection

Введение

С развитием цифровизации и увеличением объемов обмена данными в научной среде возрастает риск утечки конфиденциальной информации. Особенно остро эта проблема стоит в гуманитарных и востоковедческих исследованиях, где в обороте находятся редкие архивные документы, устные интервью и материалы полевых исследований. Традиционные средства коммуникации — электронная почта и мессенджеры — не гарантируют защиты от взломов и перехвата сообщений.

Сервис *Send.1hut.ru* разработан в качестве решения данной проблемы. Он позволяет исследователям безопасно передавать данные посредством шифрования алгоритмом AES-256-CBC[1], признанным международным стандартом (FIPS 197) и используемым для защиты секретной информации государственных структур. Алгоритм включен в Реестр российского программного обеспечения[2] и используется другими организациями в РФ. Учитывая цифровое развитие за рубежом, необходимость в защите информации академических исследований требует внимательного отношения. Система предоставляет возможность защиты информации путем кодирования шестизначный кодом, который известен только отправителю и получателю. Но при этом надо учитывать защиту речевой информации. Защита речевой информации от утечки по техническим каналам — важнейшая задача в современную цифровую эпоху. С ростом зависимости от технологий и интернета в сфере коммуникации обеспечение конфиденциальности и целостности речевой информации стало более сложной задачей, чем когда-либо прежде. И этот момент нужно учитывать при передаче кода расшифровки [1].

Принцип работы AES-256-CBC

Симметричный алгоритм блочного шифрования AES (Advanced Encryption Standard) —шифр, утверждённый Национальным институтом стандартов и технологий США[3] в 2001 г. под именем FIPS 197 [3]. В варианте AES-256 используется 256-битный ключ и 14 раундов преобразований данных. Каждый раунд включает в себя несколько этапов: подстановка байтов, перестановка строк, смешивание столбцов и добавление ключа. Эти операции делают AES устойчивым к различным видам атак, включая атаки по выбору и атаки с полным перебором.

Режим сцепления блоков шифротекста CBC (Cipher Block Chaining) — это режим шифрования, в котором каждый новый зашифрованный фрагмент данных связан с предыдущим. Для самого первого фрагмента используется случайное начальное значение — инициализационный вектор (Initialization Vector, IV[4]), — благодаря которому результат шифрования получается уникальным даже при одинаковых исходных данных. В сервисе Send.1hut.ru данные после шифрования преобразуются в кодировку Base64, что позволяет безопасно передавать их по текстовым протоколам (HTTP, email).

AES широко используется во многих областях, включая защиту данных в государственных учреждениях, финансовых организациях и при передаче информации через интернет. Его эффективность и безопасность делают его хорошим выбором для шифрования данных на различных устройствах, от мобильных теле-

---

[1] Свидетельство о государственной регистрации программы для ЭВМ № 2023681762 Российская Федерация. Программа для безопасной передачи сообщений с использованием криптографических алгоритмов: «AES-256-CBC» для шифрования текста и «RSA» для электронной подписи: № 2023680339: заявл. 06.10.2023: опубл. 18.10.2023 / Р. А. Гордеев. – EDN CFBKUV.

[2] https://reestr.digital.gov.ru/reestr/901247/

[3] National Metrology Institute for the United States, NIST

[4] Инициализационный вектор IV — это случайный набор данных (случайное число), который используется как стартовая точка при шифровании. Он нужен для того, чтобы одинаковые сообщения при каждом шифровании давали разный результат. IV не является секретным, он передаётся вместе с зашифрованным сообщением, но без него расшифровать данные не получится.

фонов до серверов. Кроме того, AES поддерживается многими протоколами безопасности, такими как SSL/TLS, что обеспечивает защиту передаваемой информации[5].

Архитектура и функционал сервиса Send.1hut.ru

Система реализована как веб-приложение, в котором весь процесс шифрования выполняется на стороне клиента — то есть в браузере пользователя. Сервер хранит только зашифрованные файлы. Ключ для расшифровки не сохраняется и передается отдельно.

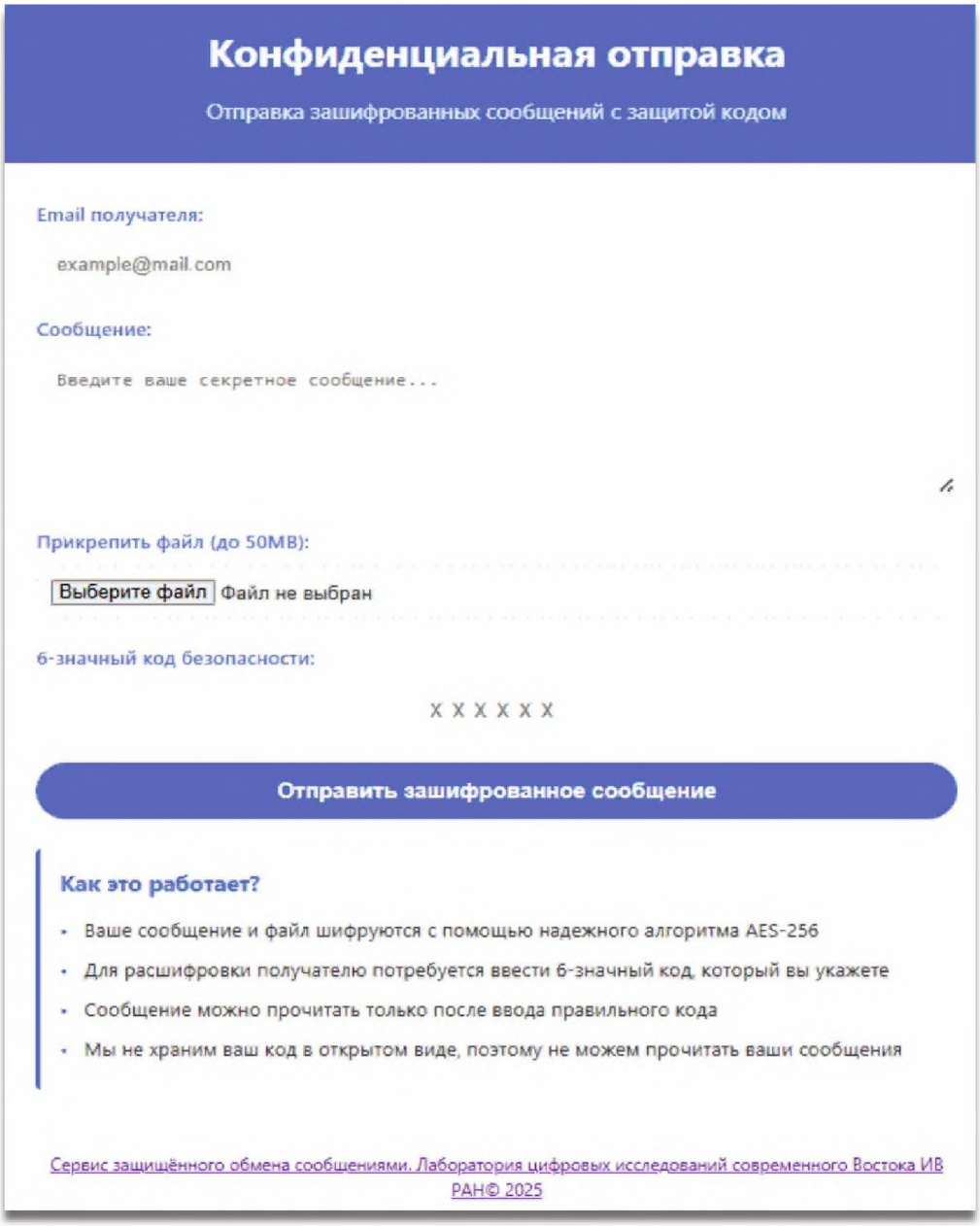

Рис. 1. Загрузка данных — интерфейс заполнения данных для отправки.

[5] https://www.ai-futureschool.com/ru/informatika/aes-sifrovanie-i-ego-primenenie.php

Процесс работы с сервисом Send.1hut.ru отличается простотой и логичностью, что делает его удобным даже для пользователей без технической подготовки. На первом этапе пользователь загружает текстовое сообщение или файл на платформу, заполняя минимальный набор полей (Рис. 1). После этого система автоматически выполняет шифрование данных по алгоритму AES-256-CBC и формирует одноразовый шестизначный код, необходимый для последующей дешифровки (Рис. 2). Далее отправителю предоставляется уникальная ссылка, которую он может переслать адресату, например, по электронной почте (Рис. 3). Получатель, перейдя по полученной ссылке, видит форму для ввода кода доступа (Рис. 4), без которого расшифровка невозможна. После ввода правильного кода система мгновенно расшифровывает сообщение и предоставляет доступ к исходному содержимому (Рис. 5). Такой пошаговый механизм обеспечивает не только высокий уровень конфиденциальности, но и защищает данные от перехвата или несанкционированного просмотра даже при компрометации электронной переписки.

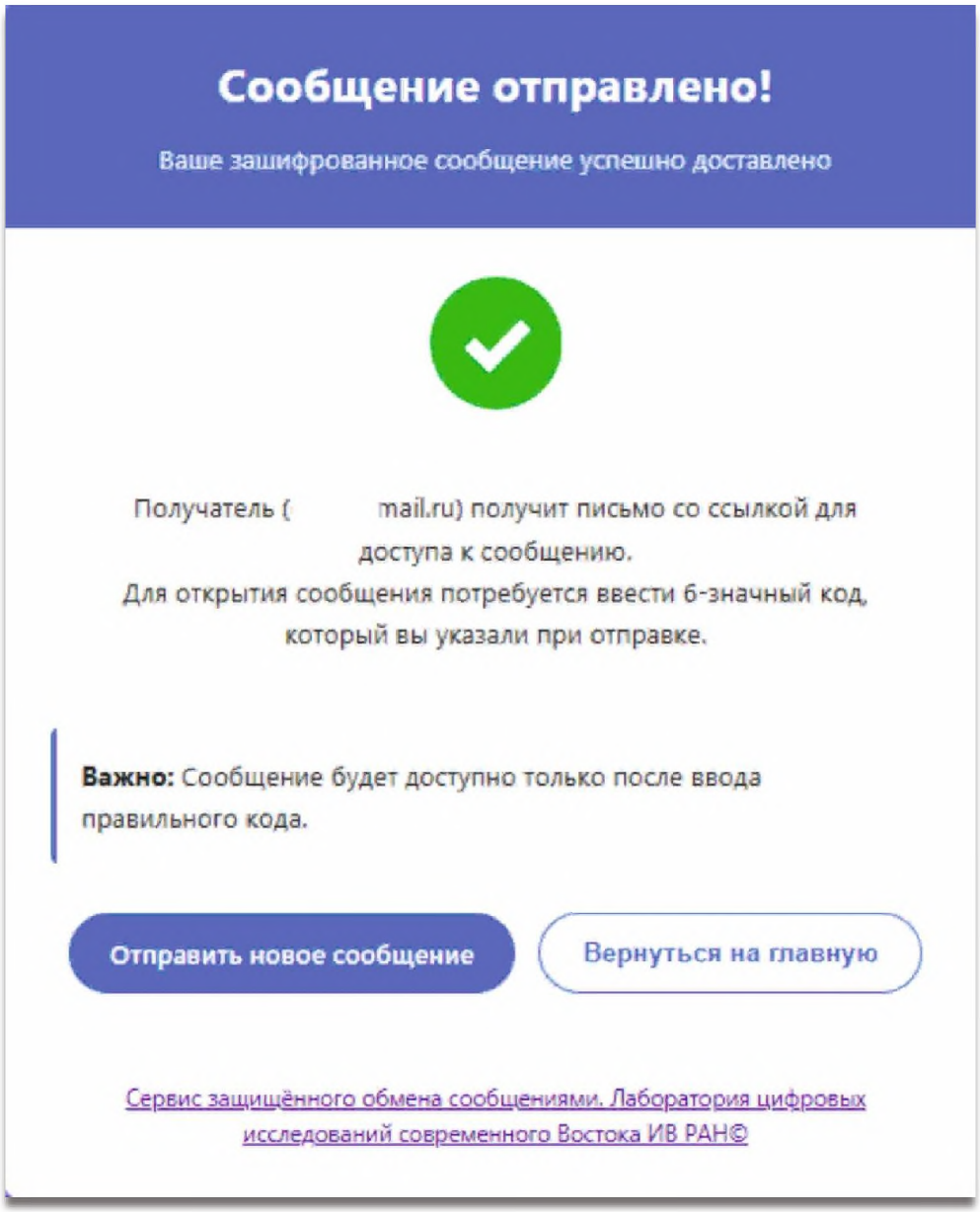

Рис. 2. Шифрование — уведомление об успешной отправке.

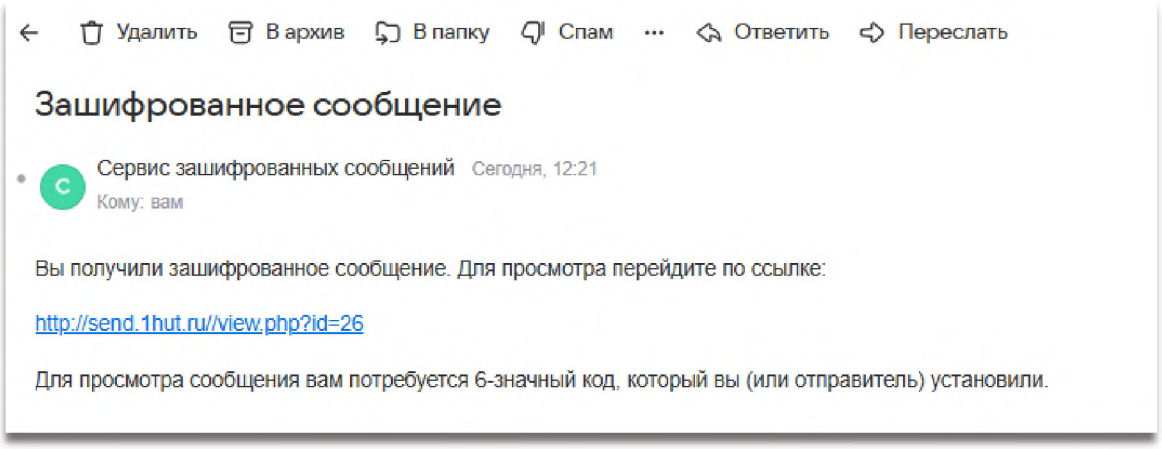

Рис. 3. Передача ссылки получателю.

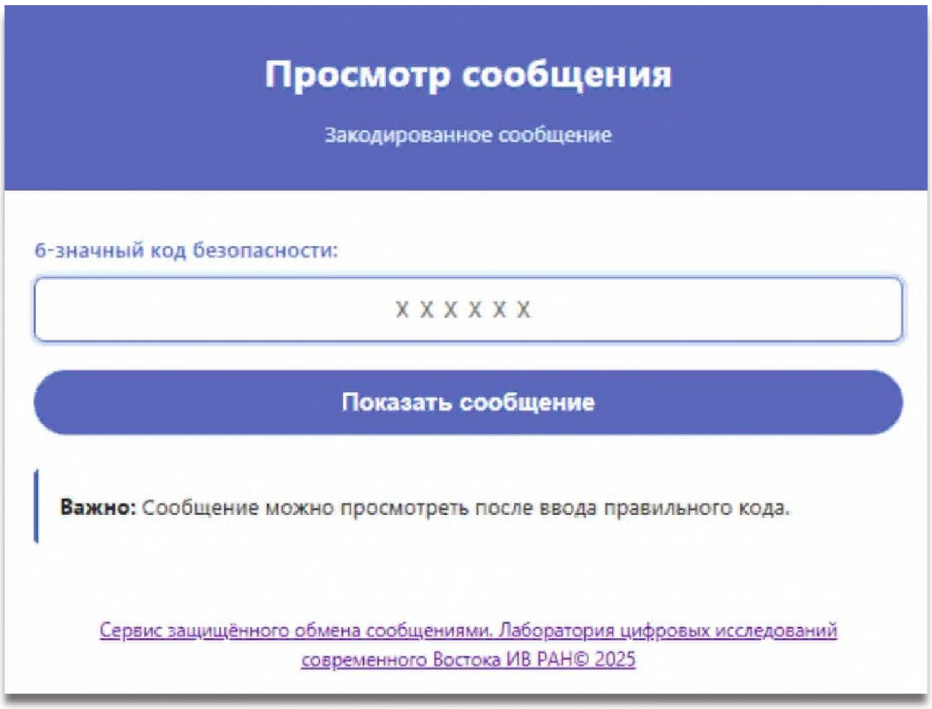

Рис. 4. Ввод кода — страница с формой ввода пароля.

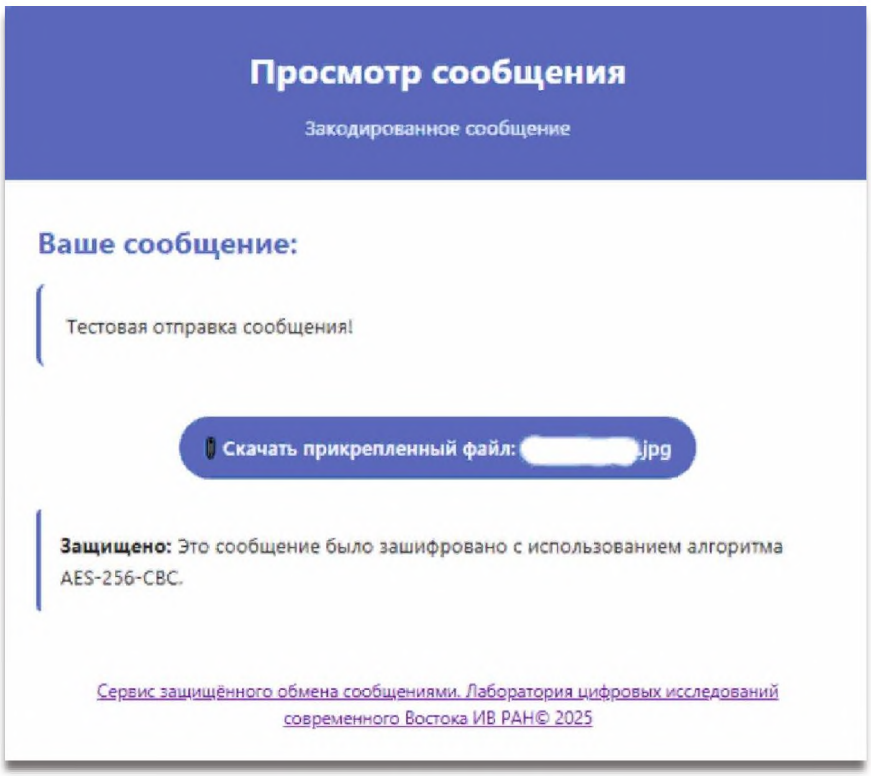

Рис. 5. Расшифровка. Результат успешного расшифрования.

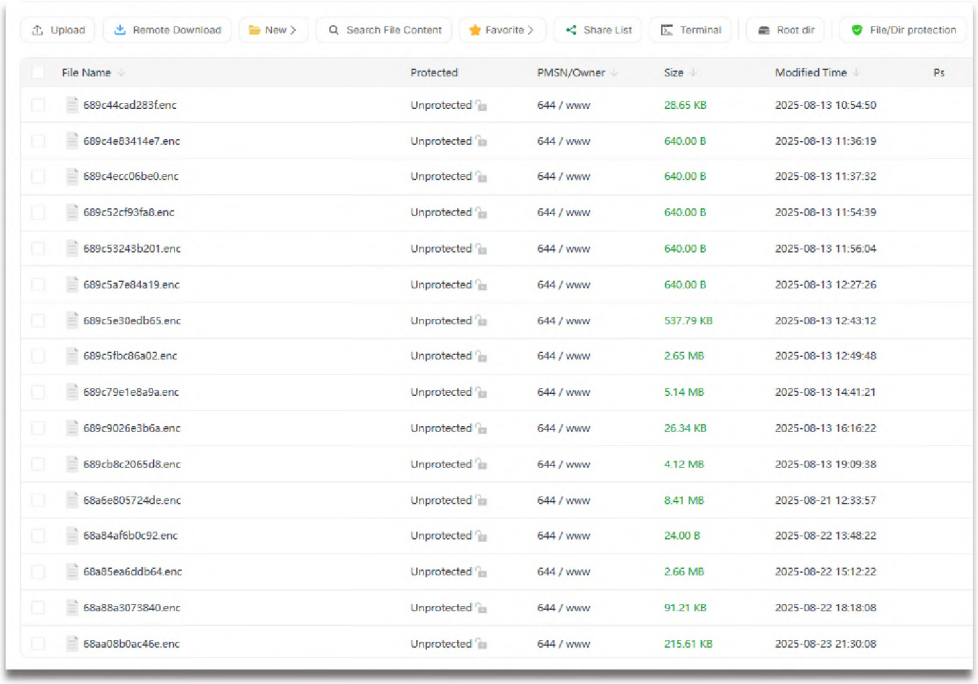

Рис. 6. Хранение файлов в формате .enc., структура зашифрованных файлов.

Применение и преимущества для научных исследований

Использование Send.1hut.ru особенно важно для учёных, работающих с конфиденциальными данными: переводами исторических текстов, полевыми интервью и анкетами, редкими архивными документами, представляющими интеллектуальную собственность.

Преимущества системы шифрования

Ключевые принципы безопасности передачи данных можно представить на примере отправки ценного письма в защищённом ящике.

Конфиденциальность обеспечивается за счёт того, что только отправитель и получатель имеют доступ к содержимому. Этот принцип реализуется с помощью шифрования, например, по алгоритму AES-256-CBC. Представьте, что ваше сообщение помещается в ящик с очень сложным замком. Открыть его можно только с помощью уникального ключа, который есть лишь у вас и у вашего адресата. Даже если этот ящик будет перехвачен во время доставки, злоумышленник не сможет прочитать его содержимое.

Целостность данных — это защита от несанкционированного изменения информации. Продолжая аналогию, представьте специальную пломбу-наклейку на этом ящике. После того как письмо помещено внутрь и замок защелкнут, на ящик наклеивается эта пломба. Если кто-то попытается вскрыть ящик в пути и изменить письмо, например, заменив сумму перевода, ему придется сорвать или повредить пломбу. Получатель, увидев поврежденную пломбу, сразу поймёт, что содержимое было изменено, и не станет доверять такому сообщению, даже если сможет открыть ящик своим ключом.

Надежность системы повышается за счёт использования специальных режимов шифрования, таких как CBC. Этот режим предотвращает предсказуемость зашифрованного текста, что существенно усложняет задачу злоумышленникам по взлому или анализу передаваемых данных.

Что касается доступности, то сервис организован таким образом, что для его использования не требуется предварительная регистрация. Интерфейс интуитивно понятен, что позволяет быстро и без лишних сложностей начать работу и обеспечить безопасную передачу информации.

Анализ рисков и угроз информационной безопасности

Несмотря на повсеместное распространение технологий шифрования, значительный объем утечек данных продолжает происходить из-за уязвимостей, сохраняющихся в традиционных каналах связи. Современные угрозы, такие как фишинг, взлом мессенджеров и компрометация почтовых ящиков, сместились с атаки на сами алгоритмы шифрования, которые зачастую оказываются практически невзламываемыми, на целевые атаки против конечных точек передачи данных и человеческого фактора.

Главной причиной сложившейся ситуации остается человеческий фактор, который превратился в основной вектор для атак. Через социальную инженерию злоумышленники добиваются значительного вредоносного эффекта, поскольку фишинг и подобные методы нацелены не на взлом программного кода, а на обман самого пользователя. Порой достаточно одного неосторожного клика по ссылке или открытия инфицированного вложения, чтобы под угрозой оказалась вся система. Эта проблема усугубляется тем, что пользователи часто не обучены распознавать уловки, используют простые пароли и пренебрегают базовыми правилами гигиены (например, повторно используют пароли на разных сервисах) [2].

Еще одним критическим источником рисков являются уязвимости, заложенные в самих платформах и протоколах связи. Зачастую корень проблемы кроется в устаревшей ИТ-инфраструктуре. Многие организации до сих пор используют

почтовые серверы и протоколы, не отвечающие современным стандартам безопасности. Яркий пример — использование протокола SMTP без обязательного шифрования, что делает передаваемые данные легкой добычей для перехвата. Даже в случае с современными мессенджерами и почтовыми клиентами нельзя исключать риски, связанные с ошибками реализации. Периодически в этом программном обеспечении обнаруживаются уязвимости, которые могут позволить злоумышленникам получить доступ к переписке или учетным данным пользователей. Отдельного внимания заслуживает растущая угроза для мобильных устройств. Поскольку мессенджеры часто используются на смартфонах, которые могут быть заражены вредоносным ПО через неофициальные магазины приложений или фишинговые сайты [4].

Дополнительные меры кибербезопасности для исследователей

В условиях цифровой трансформации науки обеспечение кибербезопасности исследовательской деятельности переходит из разряда вспомогательных функций в категорию критически важных элементов научной инфраструктуры. Реализация расширенных защитных мер направлена не только на сохранение конфиденциальности, но и на обеспечение целостности, аутентичности и доступности научных данных, что является фундаментом для соблюдения принципов академической добросовестности и защиты интеллектуальной собственности.

Методы и принципы защиты данных при хранении и передаче

Методы и принципы защиты данных при их хранении и передаче представляют собой систему взаимодополняющих мер, направленных на обеспечение конфиденциальности, целостности и доступности информации. Базовым уровнем защиты выступает полное шифрование носителей (Full-Disk Encryption, FDE), реализуемое средствами операционных систем, таких как BitLocker, FileVault или LUKS. Этот подход позволяет минимизировать риски, связанные с утратой или хищением физических устройств, и предотвращает несанкционированный доступ к данным при компрометации оборудования.

Следующий уровень защиты связан с шифрованием на уровне файловых контейнеров, что особенно важно при работе с чувствительными данными — персональными сведениями респондентов, результатами экспериментов, черновиками научных работ и неопубликованными рукописями. Для этого рекомендуется использовать создание зашифрованных виртуальных томов с помощью программных решений вроде VeraCrypt. Подобная практика реализует принцип дополнительного эшелонирования защиты, когда даже при компрометации основной системы данные внутри зашифрованного контейнера остаются недоступными.

Особое внимание должно уделяться безопасному обмену данными. Передача исследовательских материалов должна осуществляться исключительно по защищённым каналам с применением криптографических методов шифрования. Приоритет следует отдавать корпоративным платформам, предоставляемым научной организацией, поскольку они обеспечивают централизованный контроль, аудит действий и надёжное хранение данных. Если же обмен данными носит децентрализованный характер, необходимо использовать решения со сквозным шифрованием (end-to-end encryption), например, PGP для электронной почты или

специализированные мессенджеры, обеспечивающие полную конфиденциальность сообщений. В случаях передачи файлов через облачные хранилища обязательным условием является их предварительное шифрование, а передача паролей для доступа должна производиться по альтернативному, защищённому каналу связи.

Неотъемлемой частью системы защиты является стратегия резервного копирования. Для обеспечения устойчивости исследовательской инфраструктуры рекомендуется поддерживать не менее трёх копий данных: одну рабочую и две резервные. Важно использовать два различных типа носителей — например, сетевое хранилище (NAS) и облачную платформу, предпочтительно отечественного происхождения, с обязательной двухфакторной аутентификацией. Одну из копий следует размещать в географически удалённой локации, что позволит сохранить доступ к данным и обеспечить непрерывность исследовательского процесса даже в случае инцидентов или аварий на основной площадке. Таким образом, комплексная реализация перечисленных принципов создаёт надёжный многоуровневый контур защиты данных, соответствующий современным требованиям академической и информационной безопасности.

Заключение

Сервис Send.1hut.ru представляет собой важный инструмент цифровой безопасности в академической среде. Реализация шифрования AES-256-CBC обеспечивает высокий уровень защиты данных, а одноразовые коды дешифрования добавляют дополнительный слой безопасности. Решение востребовано в гуманитарных и востоковедческих исследованиях, где ценность передаваемой информации особенно высока. Реализация предложенного комплекса мер позволяет перейти от реактивной к проактивной парадигме кибербезопасности в научной деятельности. Интеграция этих практик в повседневную исследовательскую работу является не административной нагрузкой, а инвестицией в обеспечение достоверности, воспроизводимости и долгосрочной ценности научного результата.

Библиография

1. Нуриев, С. А., Карцан И. Н. Защищенность речевой информации в научных организациях от утечки по техническим каналам // Современные инновации, системы и технологии. – 2023. – Т. 3, № 4. – С. 349–362. – DOI 10.47813/2782-2818-2023-3-4-0349-0362. – EDN YBBHQM.
2. Куранов, Д. О., Полуян А. Ю. Роль человеческого фактора в обеспечении информационной безопасности // Актуальные проблемы науки и техники. 2025: Материалы Всероссийской (национальной) научно-практической конференции, посвященной 95-летию Донского государственного технического университета, Ростов-на-Дону, 12–14 марта 2025 года. – Ростов-на-Дону: Донской государственный технический университет, 2025. – С. 390.
3. Публикация федерального стандарта обработки информации США NIST FIPS 197: Advanced Encryption Standard (AES). 2001. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
4. Рудзейт, О. Ю., Добржинский Ю. В., Титанов В. М. Оценка уязвимостей протоколов передачи данных в информационных системах // Отходы и ресурсы.

2022. Т. 9. № 1. С. 1–11. https://mir-nauki.com/PDF/16ITOR122.pdf DOI: 10.15862/16ITOR122
5. Progress. Use AES-256 Encryption to Secure Data. 2022. https://www.progress.com/blogs/use-aes-256-encryption-secure-data
6. Advanced Encryption Standard (AES) implementation // GitHub. https://github.com/halloweeks/AES-256-CBC
7. Система обмена зашифрованными данными Лаборатории цифровых исследований современного Востока ИВ РАН. https://Send.1hut.ru
8. Спам и фишинг в 2025 году // https://securelist.ru/spam-and-phishing-report-2025/114623/
9. AES-256-GCM vs AES-256-CBC: What Should You Use for Secure Encryption? // Nash Tech. https://blog.nashtechglobal.com/aes-256-gcm-vs-aes-256-cbc-wh%D0%B0t-should-you-use-for-secure-encrypt%D1%96on/

References

1. Nuriev, S. A., & Kartsan, I. N. Protection of speech information in scientific organizations against leakage through technical channels. Modern Innovations, Systems and Technologies, 3(4), 2023. P. 349–361. https://doi.org/10.47813/2782-2818-2023-3-4-0349-0362
2. Kuranov, D. O., Poluyan, A. Yu. The Role of the Human Factor in Ensuring Information Security. In Current Problems of Science and Technology. 2025: Proceedings of the All-Russian (National) Research and Practice Conference Dedicated to the 95th Anniversary of Rosrov-on-Don State Technical University. March 12–14, 2025. P. 390. Rostov-on-Don: Don State Technical University.
3. Federal Information Processing Standards Publication FIPS 197: Advanced Encryption Standard (AES). 2001. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
4. Rudzeyt O.U., Dobrzhinskii U.V., Titanov V.M. Vulnerability assessment of data transmission protocols in information systems. Russian Journal of Resources, Conservation and Recycling, 9(1). P. 1–11. https://mir-nauki.com/PDF/16ITOR122.pdf DOI: 10.15862/16ITOR122
5. Progress. Use AES-256 Encryption to Secure Data. 2022. https://www.progress.com/blogs/use-aes-256-encryption-secure-data
6. Advanced Encryption Standard (AES) implementation // GitHub. https://github.com/halloweeks/AES-256-CBC
7. Encrypted Data Exchange System of the Laboratory for Digital Studies of the Contemporary East at the Institute of Oriental Studies of the Russian Academy of Sciences. https://Send.1hut.ru
8. Спам Spam and phishing in 2025 // https://securelist.ru/spam-and-phishing-report-2025/114623/
9. AES-256-GCM vs AES-256-CBC: What Should You Use for Secure Encryption? // Nash Tech. https://blog.nashtechglobal.com/aes-256-gcm-vs-aes-256-cbc-wh%D0%B0t-should-you-use-for-secure-encrypt%D1%96on/