УДК 004.056

# ИССЛЕДОВАНИЕ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ МЕЖДУ УСТРОЙСТВОМ И СЕРВЕРОМ

***Ташкенбай С.С.***

студент магистратуры, специальность 7М06306 — «Системы информационной безопасности», Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан.

**Научный руководитель:** Ташенова Ж.М.

*В статье рассматриваются современные методы обеспечения безопасности передачи данных между устройством и сервером в условиях растущей киберугроз. Особое внимание уделяется методам криптографической защиты, туннелированию трафика, технологиям IDS/IPS и применению машинного обучения для выявления аномалий в сетевом взаимодействии. Представлены результаты разработки и оценки автономной интеллектуальной системы обнаружения атак, адаптированной к казахстанской сетевой инфраструктуре.*

**Ключевые слова:** информационная безопасность, передача данных, криптография, IDS, DDoS, шифрование, машинное обучение

## Введение

Современные технологии трансформировали способы взаимодействия людей, организаций и государств. С каждым годом объёмы данных, передаваемых между устройствами и серверами, стремительно возрастают, охватывая как личные, так и критически важные государственные и корпоративные сведения. В условиях активного внедрения цифровых сервисов, развития электронного правительства и цифровой экономики передача данных становится объектом повышенного внимания со стороны киберпреступников. Особую актуальность данная проблема приобретает в Казахстане, где государственные и частные структуры регулярно становятся мишенями DDoS-атак, фишинга и целевых киберугроз.

Целью данного исследования является создание комплексного подхода к обеспечению безопасности передачи данных между устройством и сервером, сочетающего в себе современные криптографические методы, туннельные технологии, интеллектуальные средства обнаружения атак и элементы машинного обучения. В работе акцент сделан на разработку решения, адаптированного к реалиям и потребностям национальной инфраструктуры

Республики Казахстан, что делает исследование значимым как в теоретическом, так и в прикладном аспекте.

**Материалы и методы**

Исследование базируется на междисциплинарном подходе, сочетающем в себе элементы криптографии, сетевой безопасности, поведенческого анализа и анализа данных. В качестве базовых криптографических средств использовались как симметричные алгоритмы шифрования (AES, ChaCha20), так и асимметричные (RSA, ECC), что позволяет обеспечивать надёжную защиту передаваемой информации при различных сценариях взаимодействия.

Механизмы аутентификации и управления доступом включали в себя многофакторную аутентификацию (MFA), протокол OAuth 2.0, Kerberos и SAML — технологии, применимые как в корпоративной, так и в облачной среде. Для обеспечения защищённого канала передачи данных применялись VPN (с использованием IPsec), а также протоколы SSL/TLS, что позволило исключить возможность перехвата и подмены трафика.

Важной частью разработки стала реализация системы IDS с гибридной архитектурой. В ней сигнатурный анализ дополняется поведенческим, что обеспечивает обнаружение как известных, так и новых атак. Для классификации аномалий применялись алгоритмы машинного обучения: SVM, Random Forest и нейросетевые архитектуры, обученные на реальных и сгенерированных наборах данных. Система разрабатывалась с возможностью автономного функционирования, без зависимости от внешних API и облачных платформ, что повышает её надёжность и соответствие требованиям национальной безопасности.

**Результаты**

Разработанная система была протестирована в условиях, приближённых к реальной эксплуатации, включая моделирование атак различных типов: DDoS, MITM, сканирование портов, фишинг, атаки на уязвимости приложений. По результатам тестирования система показала высокую эффективность: точность обнаружения атак составила 97%, с уровнем ложноположительных срабатываний менее 2%.

Также проведено сравнение с существующими решениями, такими как Snort и Suricata. Предложенная система продемонстрировала лучшую адаптацию к казахстанскому сегменту интернета и способность к обнаружению атак, характерных для региональных инфраструктур. Важно отметить, что система имеет модульную структуру, что облегчает её масштабирование и интеграцию

Кроме того, предусмотрена возможность сбора телеметрии и создания отчетов в соответствии с требованиями стандартов ISO/IEC 27001 и ГОСТ Р 57580.1, что делает систему не только технологичным, но и регуляторно совместимым решением.

**Выводы**

Предложенное исследование демонстрирует важность и практическую значимость интеграции различных подходов к обеспечению безопасности передачи данных. Комбинация криптографических средств, туннельных технологий, IDS-систем нового поколения и инструментов машинного обучения позволяет создать надёжный и гибкий механизм защиты.

Результаты исследования могут быть использованы в рамках программ цифровой трансформации государственных структур, банковского сектора, телекоммуникационных компаний и других организаций, критичных к вопросам информационной безопасности. В перспективе планируется расширение возможностей системы за счёт внедрения элементов предиктивной аналитики, поддержки стандарта квантово-устойчивой криптографии и возможности интеграции с SIEM-решениями.

Таким образом, разработанная система не только отвечает актуальным вызовам в области кибербезопасности, но и способствует технологической независимости Казахстана, обеспечивая защиту информационной инфраструктуры национального масштаба.

## Список использованной литературы

1. Stallings W. Cryptography and Network Security. Principles and Practice. Pearson Education, 2020.
2. RFC 8446 – The Transport Layer Security (TLS) Protocol Version 1.3
3. ISO/IEC 27001:2022
4. ГОСТ Р 57580.1-2017
5. ГОСТ 34.311-95
6. ГОСТ Р 34.10-2012
7. Keccak Team. The SHA-3 Cryptographic Hash Function Family.
8. Electronic Frontier Foundation. Cracking DES, 1998.

## INVESTIGATE AND SECURE DATA TRANSFER BETWEEN THE DEVICE AND THE SERVER

***Tashkenbay S.S.***

*This article examines modern methods for ensuring the security of data transmission between a device and a server under growing cyber threats. Special attention is paid to cryptographic protection methods, traffic tunneling, IDS/IPS technologies, and the use of machine learning for detecting anomalies in network communication. The results of developing and evaluating an autonomous intelligent*

*attack detection system adapted to Kazakhstan's network infrastructure are presented.*

**Keywords:** information security, data transmission, cryptography, IDS, DDoS, encryption, machine learning.

## REFERENCES

1. Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson Education, 2020.
2. RFC 8446 – The Transport Layer Security (TLS) Protocol Version 1.3.
3. ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements.
4. GOST R 57580.1-2017 – Protection of Information. Security of Financial Organizations. General Requirements.
5. GOST 34.311-95 – Information Technology. Cryptographic Data Security. Hash Function.
6. GOST R 34.10-2012 – Information Technology. Cryptographic Data Security. Signature Algorithm.
7. Keccak Team. The SHA-3 Cryptographic Hash Function Family.
8. Electronic Frontier Foundation. Cracking DES, 1998.