УДК 004.056.5

А. А. Колпакова[1]✉

Распределенная система безопасного удаленного сетевого доступа

[1]Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: akolpakovaa@mail.ru

Аннотация. В статье рассмотрена реализация распределенной системы безопасного удаленного сетевого доступа, обеспечивающей конфиденциальность и доступность информационных ресурсов. Конфиденциальность обеспечивается использованием технологий VPN, а доступность – географически распределенными серверами, а также возможностью автоматического переключения между протоколами VPN. Использование средства управления конфигурациями Ansible позволяет не только автоматизировать процесс развертывания серверов и клиентов VPN, но и обеспечивает повторяемость и консистентность конфигураций, что также уменьшает риск возникновения ошибок ручного конфигурирования. Исследование системы проведено в соответствии с моделью угроз STRIDE. Областью применения разработанной системы является обеспечение сетевой информационной безопасности корпоративных вычислительных сетей, в частности, конечных узлов сети под управлением операционных систем семейства Linux, функционирующих на базе стека протоколов TCP/IP.

Ключевые слова: удаленный доступ, распределенные системы, автоматизированное конфигурирование, VPN, Ansible

A. A. Kolpakova[1]✉

Distributed Secure Remote Network Access System

[1]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Moscow, Russian Federation
e-mail: akolpakovaa@mail.ru

Abstract. The article considers the realization of a distributed system of secure remote network access that provides confidentiality and availability of information resources. Confidentiality is provided by using VPN technologies, and availability - by geographically distributed servers, as well as the ability to automatically switch between VPN protocols. The use of Ansible configuration management tool allows not only to automate the process of deployment of VPN servers and clients, but also provides repeatability and consistency of configurations, which also reduces the risk of manual configuration errors. The system has been studied in accordance with the STRIDE threat model. The application area of the developed system is to ensure network information security of corporate computer networks, in particular, network endpoints under the control of operating systems of Linux family, operating on the basis of TCP/IP protocol stack.

Keywords: remote access, distributed systems, automated configuration, VPN, Ansible

Введение

В настоящее время организация удаленного доступа к корпоративной информационной инфраструктуре представляет собой ключевой аспект обеспечения непрерывности бизнес-процессов. Возможность администрирования информационных ресурсов вне зависимости от территориального расположения пользователя

способствует оптимизации рабочих процессов и повышению общей эффективности деятельности организаций.

Следует отметить, что технологиям обеспечения удаленного сетевого доступа присущ ряд недостатков, включая потенциальные угрозы безопасности, приводящие к возможности получения несанкционированного доступа к данным, а также наличие вероятных проблем, связанных с сетевой доступностью и производительностью.

На сегодняшний день рынок предлагает широкий спектр коммерческих решений от известных разработчиков, таких как TeamViewer, AmmyyAdmin и AnyDesk. Тем не менее, анализ данных программных продуктов выявляет наличие различных уязвимостей, подобных CVE 2021-34803 в TeamViewer, позволяющей загружать недоверенные DLL-библиотеки [1]. Существенный временной промежуток между обнаружением уязвимостей и выпуском исправлений, особенно в корпоративном сегменте, где требуется многоступенчатое тестирование обновлений, создает дополнительные риски. Вследствие этого, а также в связи с уходом ряда зарубежных компаний с российского рынка, появляется необходимость в разработке отечественных программных решений.

Проблематика обеспечения безопасного удаленного доступа активно исследуется как российскими, так и зарубежными специалистами. В научных работах [2, 3] детально рассматриваются методы организации удаленного взаимодействия через протоколы SSH и RDP, однако недостаточно внимания уделяется технологиям виртуальных частных сетей (VPN). Перспективным направлением защиты является использование технологии Port Knocking, которой посвящен ряд исследований [4–8].

Значительный интерес представляют оверлейные технологии, обеспечивающие анонимность при удаленном взаимодействии. Данное направление активно развивается научной школой «Сетевая информационная безопасность» под руководством Басыни Е. А. [9–11]. Отдельного изучения заслуживают методы детектирования VPN и средств анонимизации [12–18], что подчеркивает необходимость совершенствования механизмов защиты данных при удаленном доступе.

На основании представленной проблематики предметной области становится возможным сделать вывод, что в настоящее время возрастает актуальность в разработке решений, обеспечивающих защищенный удаленный доступ в условиях потенциальной компрометации данных на магистральных линиях связи.

Постановка задачи

Целью настоящей работы является разработка системы, обеспечивающей конфиденциальность и доступность информационных ресурсов при удаленном доступе на базе стека протоколов TCP/IPv4 для операционных систем семейства Linux.

В ходе работы была проведена ее декомпозиция на следующие задачи:

1) исследование предметной области;
2) моделирование предметной области;

3) проектирование распределенной системы безопасного удаленного сетевого доступа;

4) программная реализация спроектированной системы безопасного удаленного сетевого доступа;

5) тестирование и исследование реализованного решения.

Предлагаемое решение

Распределенная система удаленного доступа основана на различных технологиях VPN для повышения конфиденциальности и использует систему управления конфигурации Ansible, которая обеспечивает повторяемость и консистентность конфигураций. Доступность системы достигается использованием физически разнесенных серверов OpenVPN и WireGuard, а также автоматическим переключением соединения к другой технологии при недоступности первой.

Система (рис. 1) состоит из нескольких важных частей: клиентское ПО (или клиент), VPN-сервера и серверное ПО (или центр управления). C4-диаграмма демонстрирует взаимодействие различных компонент распределенной системы, что позволяет различным группам участников проектирования, разработки и эксплуатации системы получить необходимый объем информации, соответствующий их роли. C4 в названии расшифровывается как четыре уровня диаграмм: Context (Контекст), Container (Контейнер), Component (Компонент) и Code (Код).

Рис. 1. Контекстная диаграмма разрабатываемого решения

Более детально архитектуру системы отображает компонентная диаграмма (рис. 2). Диаграмма демонстрирует ключевые компоненты, их функциональность и взаимодействие между собой, а также связь с внешними участниками, такими как администратор и клиенты.

Одной из основных функций системы является возможность развертывания сервера VPN с помощью Ansible-плейбуков. Такой процесс позволяет администраторам системы эффективно разворачивать новые серверы.

Диаграмма последовательности (рис. 3) демонстрирует процесс автоматизации развертывания VPN серверов, включая проверку входных данных, выполнение конфигурационных сценариев и взаимодействие с базой данных. Это упрощает развертывание новых серверов, повышает надежность операций и минимизирует возможность ошибок, связанных с ручной настройкой.

Другим важным процессом является переключение клиента на другой протокол. Диаграмма последовательности переключения протокола VPN (рис. 4) иллюстрирует процесс изменения VPN-протокола в системе, включающей взаимодействие между клиентом VPN, сервером WebSocket, сервером конфигураций (API), графическим интерфейсом (GUI) и системными процессами.

Основная цель этой диаграммы – показать, как происходит управление сменой протокола на уровне взаимодействия компонентов.

Проектирование архитектуры и формализация алгоритмов помогают структурировать процессы, определить роли и ответственность каждого элемента системы, что особенно важно для обеспечения безопасности и масштабируемости. Использование таких инструментов, как Ansible, позволяет автоматизировать рутинные задачи, минимизировать человеческий фактор и повысить эффективность администрирования.

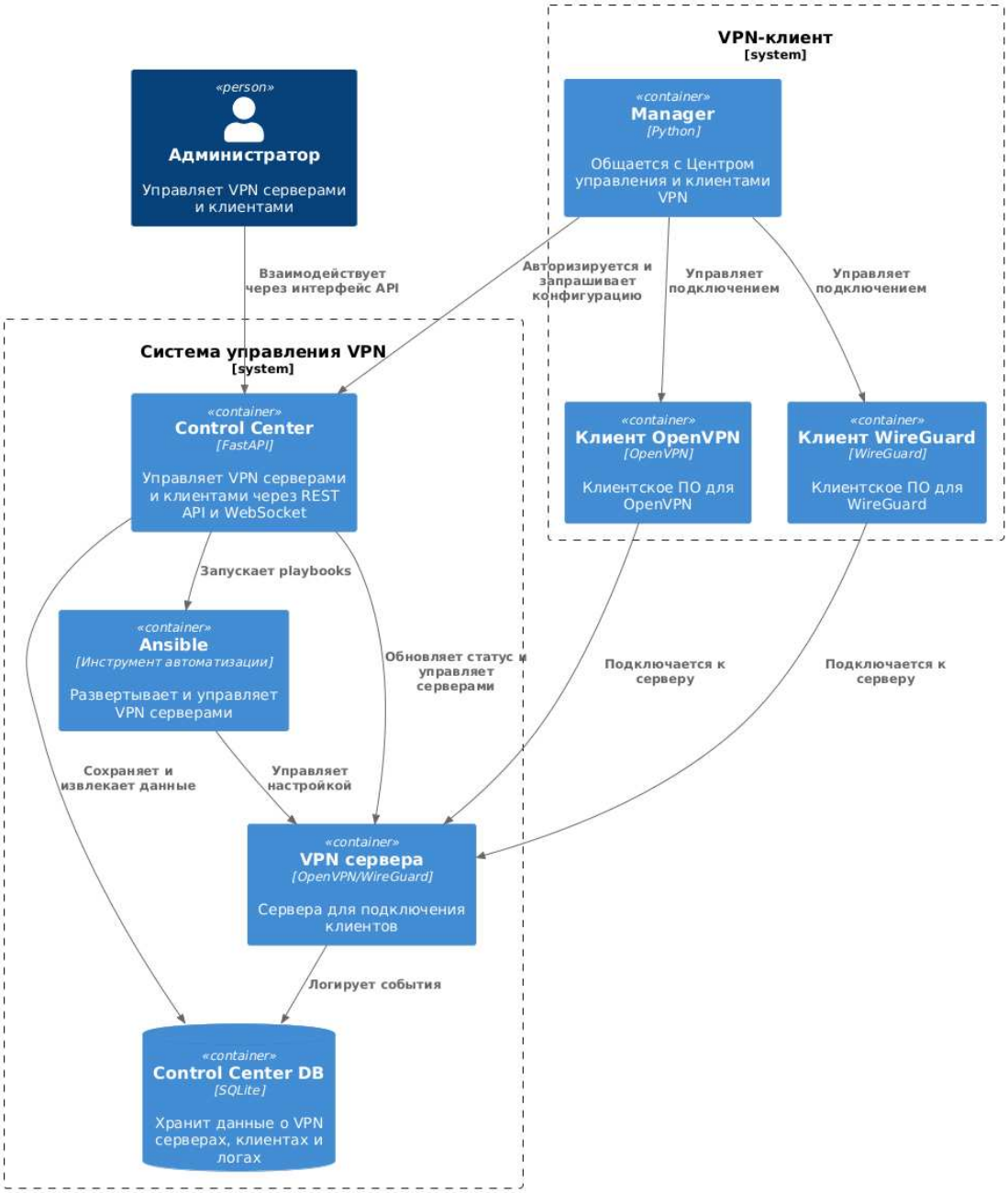

Рис. 2. Компонентная диаграмма разрабатываемого решения

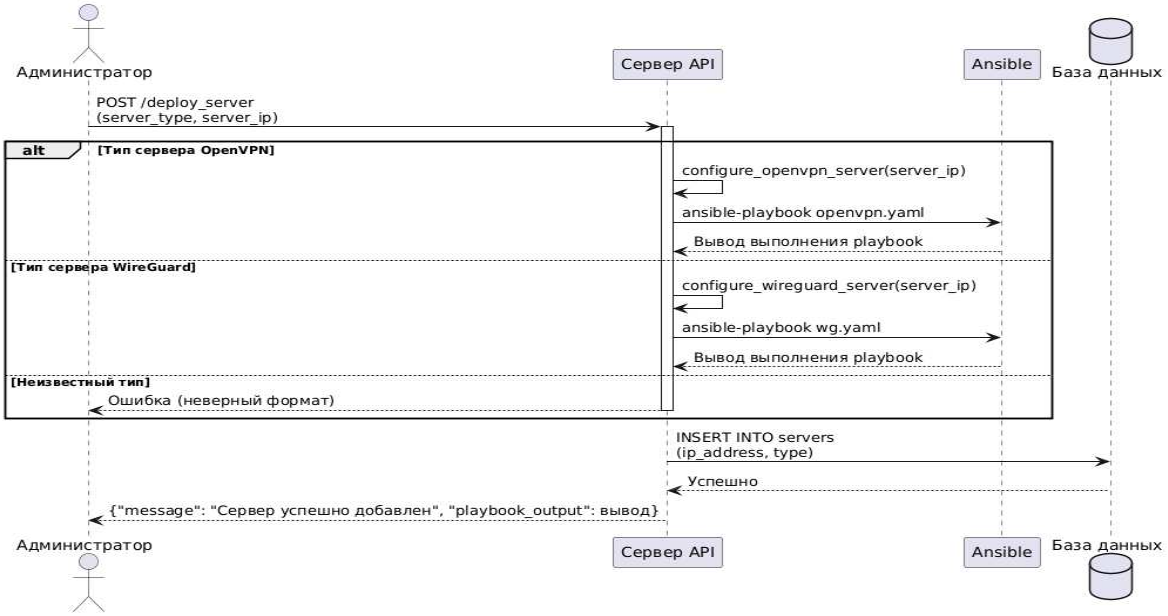

Рис. 3. Диаграмма последовательности развертывания VPN-сервера

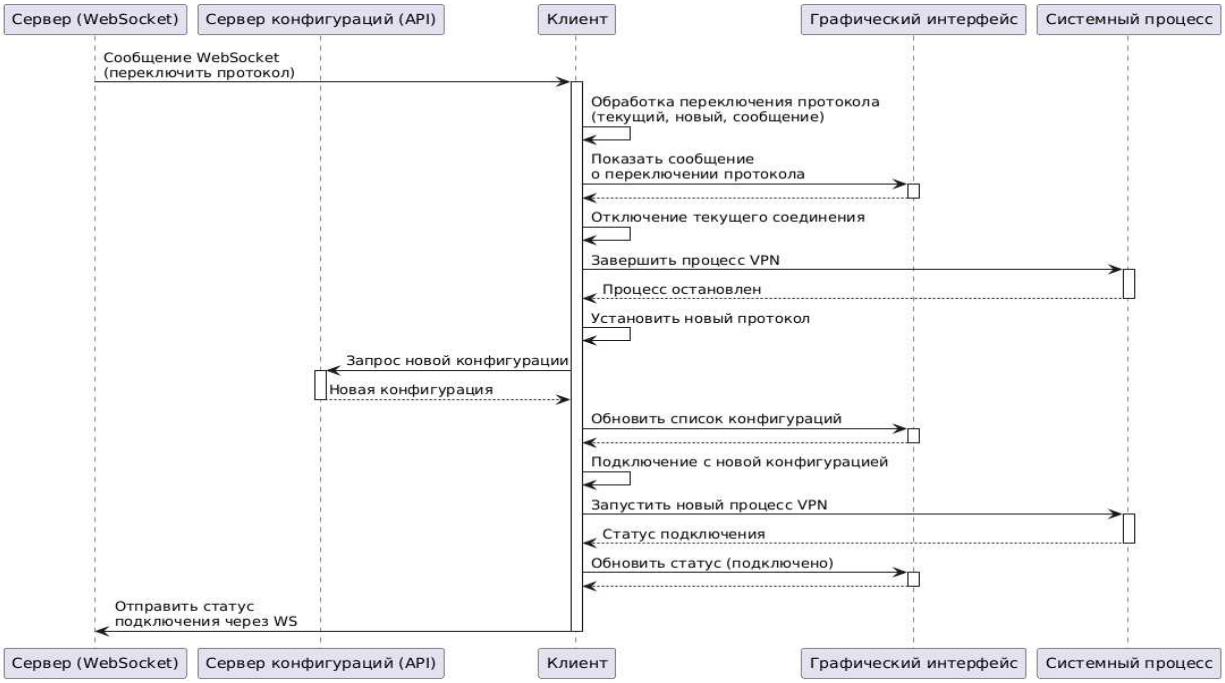

Рис. 4. Диаграмма последовательности переключения протокола VPN

Тестирование

В данной работе для демонстрации работоспособности и корректности предложенного решения проводилось ручное и автоматизированное тестирование системы, а также был проведен анализ защищенности системы управления VPN-инфраструктурой в рамках модели угроз STRIDE.

При ручном тестировании выполняются два сценария: клиент запрашивает конфигурацию с сервера и подключается к VPN-серверу, при подключении происходит

ошибка подключения и клиент автоматически подключается к другому протоколу. Стоит отметить, что клиентское ПО работает как на операционной системе Windows, так и на операционной системе Linux. Подключение происходит к серверам Linux. При неуспешном подключении клиент получает сообщение от сервера (рис. 5) о необходимости переключения на другой протокол.

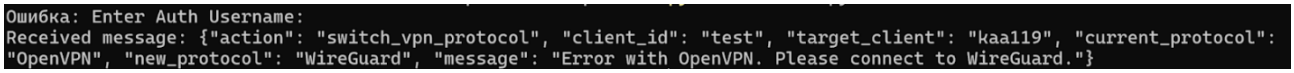

Рис. 5. Получение сообщения о смене протокола

Одной из важных составляющих частей распределенной системы удаленного сетевого доступа являются Ansible-роли для развертывания VPN-серверов. Именно поэтому особое внимание уделялось автоматическому тестированию ролей Ansible с использованием фреймворка Molecule. При тестировании выполнялось два сценария: первоначальная установка сервера (рис. 6) и проверка свойства идемпотентности (рис. 7). Данный процесс позволяет проверить корректность работы различных конфигураций и ролей, а также выявить возможные ошибки или несоответствия требованиям перед внедрением изменений в рабочую среду.

Рис. 6. Применение роли

Рис. 7. Свойство идемпотентности

В рамках разработки системы управления VPN-инфраструктурой проведен анализ защищенности в соответствии с моделью угроз STRIDE.

Угроза подделки (Spoofing) частично нейтрализуется использованием JWT-токенов с секретным ключом и HTTPS-шифрования, однако для усиления защиты требуется внедрение многофакторной аутентификации (MFA). Это позволит исключить риск фишинга и MITM-атак, а интеграция подхода Zero Trust Network Access (ZTNA) обеспечит проверку каждого запроса к критическим ресурсам.

Противодействие несанкционированному изменению данных (Tampering) реализовано через параметризованные SQL-запросы, но для полного устранения рисков модификации трафика или WebSocket-сообщений необходимы дополни-

тельные меры: внедрение HMAC для контроля целостности файлов, использование неизменяемых логов.

Противодействие угрозам отказа от действий (Repudiation) реализуется за счет базового логирования событий в SQLite, однако для обеспечения неопровержимого аудита требуется централизованная система сбора логов на базе ELK Stack и их подпись, например, RSA-4096. Это предотвратит удаление или фальсификацию записей.

Риски утечки конфиденциальных данных (Information Disclosure) минимизируются за счет TLS 1.3 и изоляции конфигурационных файлов, но для защиты от продвинутых атак необходимо внедрение DLP-систем и запуск сервисов в изолированных контейнерах. Дополнительное шифрование журналов AES-256-GCM исключит утечку данных через логи.

Угрозы отказа в обслуживании (Denial of Service) минимизируются с помощью rate limiting на API Gateway, однако для устойчивости к масштабным DDoS-атакам требуется развертывание WAF, балансировка нагрузки через HAProxy.

Повышение привилегий (Elevation of Privilege) частично покрывается проверкой прав, но для полного устранения рисков необходимы системы обнаружения вторжений (Suricata), регулярный аудит прав доступа и использование OAuth2.

К числу непокрытых угроз относится подделка клиентских сертификатов VPN, требующая внедрения mTLS, а также отсутствие механизмов автоматической ротации секретов, что повышает риски долгосрочной компрометации.

Заключение

В рамках данной работы была предложена распределенная система безопасного удаленного сетевого доступа с обеспечением конфиденциальности и доступности информационных ресурсов, которая была реализована программно и успешно протестирована.

Теоретическая значимость работы заключается в проектировании распределенных систем, обеспечивающих безопасность процесса удаленного сетевого взаимодействия, которые могут быть в дальнейшем использованы в средах, функционирующих на базе стека протоколов TCP/IP.

Практическая значимость заключается в обеспечении безопасности сетевой коммуникации при удаленном доступе, что позволяет снизить риск нанесения ущерба сетевой инфраструктуре предприятия путем предотвращения широкого спектра угроз.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. CVE-2021-34803. – URL: https://nvd.nist.gov/vuln/detail/CVE-2021-34803 (дата обращения: 22.03.2025)

2. Павлов А. Н., Гладков А. Н. Разработка методики организации удаленного управления АРМ в соединении // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. – 2021. – № 12/2. – С. 29-35

3. Ворожейкин Д.С., Кондратьев В.Ю. Исследование сетевого протокола прикладного уровня secure shell // Инновации и инвестиции. – 2020. – № 6.

4. Rajaboevich G. S., Bakhadirovna M. M., Abdulatipovich I. A. Port-Knocking Method For Enhancing Network Security //2022 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2022. – С. 1-4.

5. Pali I., Amin R. PortSec: Securing Port Knocking System using Sequence Mechanism in SDN Environment //2022 International Wireless Communications and Mobile Computing (IWCMC). — 2022. — С. 1009-1014.

6. Zidan A., Amin K. M., Ghanem T. Enhanced User Authentication Based on Dynamic Port Knocking Technique //IJCI. International Journal of Computers and Information. – 2021. – Т. 8. – № 2. – С. 115-124.

7. Junquera-Sanchez J. et al. C-Lock: Local Network Resilient Port Knocking System Based on TOTP //Wireless Communications and Mobile Computing. – 2022. – Т. 2022.

8. Bokhari A. H. et al. Empirical Analysis of Security and Power-Saving Features of Port Knocking Technique Applied to an IoT Device //Journal of Information Processing. – 2021. – Т. 29. — С. 572-580.

9. Басыня Е. А. Система самоорганизующегося виртуального защищенного канала связи / Е. А. Басыня // Защита информации. Инсайд. – 2018. – № 5 (83). – С. 10–15.

10. System of a self-organizing virtual secure communication channel based on stochastic multilayer encryption and overlay technologies / E. A. Basinya, Z. B. Akhayeva, D. H. Omarkhanova, G. B. Tolegenova [et al.]. – Text : direct // Journal of Theoretical and Applied Information Technology. – 2022. – Vol. 100, iss. 16. – P. 4918-4927.

11. Басыня Е. А. Программная реализация и исследование системы интеллектуально-адаптивного управления информационной инфраструктурой предприятия / Е. А. Басыня // Вестник Самарского государственного технического университета. Серия: Технические науки. – 2020. – Т. 28, № 1 (65). – С. 6-21.

12. Лапшичев В. В., Макаревич О. Б. Метод обнаружения и идентификации данных сети tor анализатором Wireshark //Вопросы кибербезопасности. — 2021. — № 4 (44). — С. 73-80.

13. Miller S., Curran K., Lunney T. Detection of virtual private network traffic using machine learning //International Journal of Wireless Networks and Broadband Technologies (IJWNBT). – 2020. – Т. 9. – № 2. – С. 60-80.

14. Zain ul Abideen M., Saleem S., Ejaz M. Vpn traffic detection in ssl-protected channel //Security and Communication Networks. – 2019. – Т. 2019. – С. 1-17.

15. Talkington J., Dantu R., Morozov K. Detecting Devices and Protocols on VPN-Encrypted Networks //2020 Sixth International Conference on Mobile And Secure Services (MobiSecServ). – IEEE, 2020. – С. 1-8.

16. Jan J. Detection of VPN traffic using automaton : дис. – Czech University of Technology Prague. Calculation and Information Centre, 2023.

17. Sun W. et al. A deep learning-based encrypted VPN traffic classification method using packet block image //Electronics. – 2022. – Т. 12. – № 1. – С. 115.

18. Al-Fayoumi M., Al-Fawa'reh M., Nashwan S. VPN and Non-VPN Network Traffic Classification Using Time-Related Features //Computers, Materials & Continua. – 2022. – Т. 72. – № 2.