УДК 528.71

Д. И. Касьяненко[1]*

Система автоматизированной настройки виртуальных защищенных каналов связи

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: novodanilsk@gmail.com

Аннотация. В статье рассматривается система автоматизированной настройки виртуальных защищенных каналов связи, ориентированная на обеспечение безопасности и эффективности сетевых соединений. Обсуждается проблема сложности управления сетевой безопасностью в условиях растущего числа киберугроз и многообразия сетевых технологий. Целью исследования является разработка системы, которая автоматизирует настройку и управление виртуальными защищенными каналами связи с минимальным вмешательством человека. В работе также проводится анализ уязвимостей базовых протоколов стека TCP/IP, осуществляется выбор стека технологий и разрабатывается программное обеспечение. В результате исследования разработана и представлена система автоматизированной настройки виртуальных защищенных каналов связи, призванная решить проблемы сетевой безопасности в современной информационной среде. Автоматизация процесса настройки и управления виртуальными каналами связи сокращает риски возникновения уязвимостей и повышает уровень защиты информации, что делает данную систему важным инструментом в области кибербезопасности.

Ключевые слова: Ansible, VPN, network security

D. I. Kasyanenko[1]*

System for Automated Configuration of Virtual Secure Communication Channels

[1] National Research Nuclear University MEPhI, Moscow, Russian Federation
* e-mail: novodanilsk@gmail.com

Abstract. The article discusses an automated system for configuring virtual secure communication channels, aimed at ensuring the security and efficiency of network connections. It addresses the complexity of managing network security in the face of increasing cyber threats and diverse network technologies. The research aims to develop a system that automates the configuration and management of virtual secure communication channels with minimal human intervention. The work also includes an analysis of vulnerabilities in basic TCP/IP protocols, the selection of technology stacks, and the development of software. As a result of the research, a system for automated configuration of virtual secure communication channels is developed and presented, intended to address network security challenges in the modern information environment. Automating the process of configuring and managing virtual channels reduces the risks of vulnerabilities and enhances information security, making this system an important tool in the field of cybersecurity.

Keywords: Ansible, VPN, network security

Введение

Современные компьютерные сети постоянно развиваются, сталкиваясь с растущими объемами данных и разнообразием используемых технологий. Эти тенденции отражаются в разных сферах, включая промышленные сети с множеством различных устройств, а также в концепции расширенной сети, направленной на массовое взаимодействие устройств в сети.

Вместе с преимуществами увеличение сложности компьютерных сетей представляет определенные вызовы. Большие и разнообразные сети предоставляют потенциально большую поверхность для кибератак, а разнообразие сетевых устройств усложняет обнаружение уязвимостей и управление безопасностью сети. В такой среде обеспечение эффективной сетевой безопасности становится приоритетной задачей для организаций и предприятий.

С учетом нарастающей угрозы кибератак и важности обеспечения безопасности информационной инфраструктуры, правительство Российской Федерации приняло Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который вводит дополнительные меры по защите критически важных информационных систем и предотвращению киберугроз.

В 2023 году более 90 % компаний столкнулись с утечками корпоративных учетных записей, что подчеркивает нарастающую угрозу для бизнеса. Уязвимости на периметре обнаружены у 72 % компаний, что может послужить входной точкой для атаки на инфраструктуру. Проблема проникновения через подрядные организации оказалась особенно острой, став причиной каждого пятого значимого инцидента. С учетом системного усложнения методов кибератак, включая применение искусственного интеллекта и многосоставных цепочек взлома, бизнесу предстоит столкнуться с еще большим вызовом в обеспечении киберустойчивости в 2024 году. Поэтому повышение внимания к управлению рисками цепочки поставок и инвестиции в киберстрахование станут приоритетами для бизнеса в ближайшем будущем [1].

Традиционно настройка и управление функциями безопасности в компьютерных сетях осуществляются вручную, что подвержено ошибкам и неэффективно в условиях быстро меняющейся среды угроз. В свете этого недавние исследования и разработки в области автоматизации настройки сетевой безопасности предлагают новый подход к решению этой проблемы. Основная цель этих исследований заключается в создании систем, способных автоматически настраивать и управлять функциями безопасности сети, минимизируя человеческое вмешательство [2, 3].

С учетом этого контекста эта статья фокусируется на системе автоматизированной настройки виртуальных защищенных каналов связи. В ней анализируются мотивация, преимущества и методы автоматизации сетевой безопасности, сосредотачиваясь на роли и эффективности системы виртуальных защищенных каналов связи в этом процессе. В работе предлагается обзор современного состояния этой системы, обсуждаются ключевые исследования и направления разви-

тия в этой области, а также рассматриваются возможные применения и выгоды в контексте современных требований к безопасности сетей.

Исследование предметной области

Стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol) является фундаментальной основой современных компьютерных сетей. Он состоит из четырех основных уровней: прикладной, транспортный, сетевой и канальный. Каждый уровень выполняет свои функции, обеспечивая передачу данных от отправителя к получателю. Однако вместе с распространением сетевых технологий возникают и угрозы безопасности, связанные с каждым уровнем стека протоколов TCP/IP [4–6].

На канальном уровне происходит передача данных через физическую среду, например, по Ethernet-кабелю или Wi-Fi. Здесь работают протоколы, такие как Ethernet, Wi-Fi, Bluetooth и другие. Атаки на этом уровне могут включать в себя перехват данных через подслушивание (sniffing), атаки на MAC-адреса (MAC spoofing) и физические атаки на сетевое оборудование.

Сетевой уровень управляет маршрутизацией данных в сети. Протокол IP является ключевым протоколом на этом уровне. Существуют также протоколы ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol) и другие. Атаки на этом уровне могут включать в себя атаки переполнения буфера (buffer overflow), атаки отказа в обслуживании (Denial of Service, DoS) и атаки с отравлением маршрутизации (routing poisoning).

Следующий, транспортный уровень, обеспечивает надежную передачу данных между устройствами. Протоколы TCP и UDP (User Datagram Protocol) работают на этом уровне. Атаки на этом уровне могут включать в себя атаки переполнения буфера, атаки с отказом в обслуживании и атаки на уязвимости в реализации протоколов.

На последнем прикладном уровне происходит взаимодействие приложений. Протоколы HTTP (HyperText Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), DNS (Domain Name System) и многие другие работают на этом уровне. Атаки на прикладном уровне могут включать в себя атаки по перехвату данных, внедрение злонамеренного кода (injection attacks), а также атаки на слабые места в приложениях.

Понимание работы стека протоколов TCP/IP позволяет эффективно обеспечивать безопасность сети. Отслеживание трафика на каждом уровне позволяет выявлять аномалии и потенциальные угрозы. Развертывание мер защиты на всех уровнях стека протоколов TCP/IP становится ключевым для обеспечения безопасности сети.

В условиях повсеместного использования интернета и распространения цифровых технологий безопасная передача данных между удаленными точками становится критически важной. Виртуальные частные сети (VPN) предоставляют механизм для защищенного соединения между устройствами через общедоступные сети, такие как интернет.

VPN шифруют данные перед отправкой и дешифруют их на приемном конце, обеспечивая конфиденциальность и целостность информации. Это позволяет пользователям обмениваться данными через незащищенные сети, сохраняя при этом приватность и безопасность [7, 8].

С ростом объема цифровой информации и угроз безопасности в интернете, использование VPN становится необходимостью для защиты конфиденциальных данных и обеспечения безопасного доступа к сетевым ресурсам. Особенно важно использование VPN при работе с общедоступными Wi-Fi сетями, в удаленной работе и при передаче конфиденциальной информации.

Виртуальные частные сети (VPN) играют ключевую роль в обеспечении безопасности в условиях распределенной работы и постоянного доступа к интернету. Понимание принципов работы VPN и мер безопасности на уровне стека протоколов TCP/IP позволяет организациям эффективно защищать свои сетевые ресурсы и данные в современной цифровой среде [9].

Система автоматизированной настройки виртуальных защищенных каналов связи играет ключевую роль в обеспечении безопасности сетевых коммуникаций. Она позволяет эффективно управлять защищенными каналами связи и настраивать их, минимизируя риск возможных угроз безопасности.

Существуют программные решения, такие как Ansible Tower и AWX, с помощью которых возможна автоматизированная настройка VPN. Также эти инструменты значительно упрощают процесс автоматизации настройки и управления виртуальными защищенными каналами связи. Ansible Tower имеет ограничения доступности из-за своей платной лицензии, а также требует выделенного оборудования или виртуальной машины для работы. AWX, хоть и бесплатный, сложен в установке и настройке, а также имеет ограниченные возможности масштабирования при работе с большими инфраструктурами.

Постановка задачи

Целью исследования является разработка системы автоматизированной настройки виртуальных защищенных каналов связи, обеспечивающей конфиденциальность и целостность передаваемой информации по сети.

Декомпозиция цели на задачи:

- исследование предметной области;
- выбор технологического стека;
- программная реализация предложенного решения (MVP).

Выбор стека технологий

При разработке системы автоматизированной настройки виртуальных защищенных каналов связи был проведен тщательный анализ различных технологических решений для обеспечения эффективности, масштабируемости и безопасности. В результате выбор был сделан в пользу следующего стека технологий.

Язык программирования Go: одним из ключевых решений стал выбор языка программирования Go для реализации системы. Go обладает рядом преиму-

ществ, таких как высокая производительность, простота разработки, масштабируемость и широкая поддержка сообщества. Благодаря своей компилируемой природе, Go позволяет создавать быстрые и надежные приложения, а также обеспечивает удобство в поддержке и сопровождении кода [10, 11].

База данных MySQL: для хранения и управления данными выбор был сделан в пользу MySQL. MySQL – широко используемая реляционная база данных с отличной производительностью, надежностью и гибкостью. Возможности по масштабированию и высокая доступность делают ее идеальным выбором для хранения конфигурационных данных и журналов системы [12].

Автоматизация Ansible Playbook: для автоматизации развертывания и управления системой был выбран Ansible Playbook. Ansible предоставляет простой и гибкий способ управления конфигурацией и оркестрацией приложений, а также обеспечивает удобное взаимодействие с инфраструктурой. Декларативный подход и простая конфигурация делают его идеальным инструментом для настройки и управления виртуальными защищенными каналами связи [13].

VPN-серверы OpenVPN и WireGuard: для обеспечения безопасного и защищенного соединения между удаленными сетями были выбраны OpenVPN и WireGuard. OpenVPN – широко используемое решение для создания виртуальных частных сетей с открытым исходным кодом, обеспечивающее надежное шифрование и аутентификацию. При это WireGuard представляет собой современное и легковесное решение для создания безопасных туннелей, обладающее высокой производительностью и простотой настройки. Оба решения были выбраны в силу своих надежности, производительности и простоты использования, что позволяет обеспечить высокий уровень безопасности и эффективности виртуальных защищенных каналов связи [14, 15].

Предлагаемое решение

Основой предлагаемого решения является база данных, разработанная для хранения и управления информацией о проектах, задачах, ресурсах и других сущностях, необходимых для успешного выполнения проектов. База данных будет состоять из следующих таблиц (рис. 1).

Таблица project: содержит информацию о проектах, их создании и основных настройках, таких как имя проекта.

Таблица project__repository: содержит информацию о месте хранения проектов. Связана с таблицей project через поле project_id.

Таблица project__template: содержит информацию о шаблонах задач, которые могут быть назначены в рамках проекта. Связана с таблицей project через поле project_id.

Таблица task: содержит информацию о задачах, их статусе, времени выполнения и других параметрах. Связана с таблицей project__template через поле template_id.

Таблица project__user: содержит информацию о пользователях проекта и их ролях. Связана с таблицей project через поле project_id.

Таблица event: записывает события, связанные с проектами, такие как создание проекта или выполнение задачи. Связана с таблицей project через поле project_id.

Таблица project__environment: содержит информацию об окружениях проекта, которые могут использоваться в задачах. Связана с таблицей project через поле project_id.

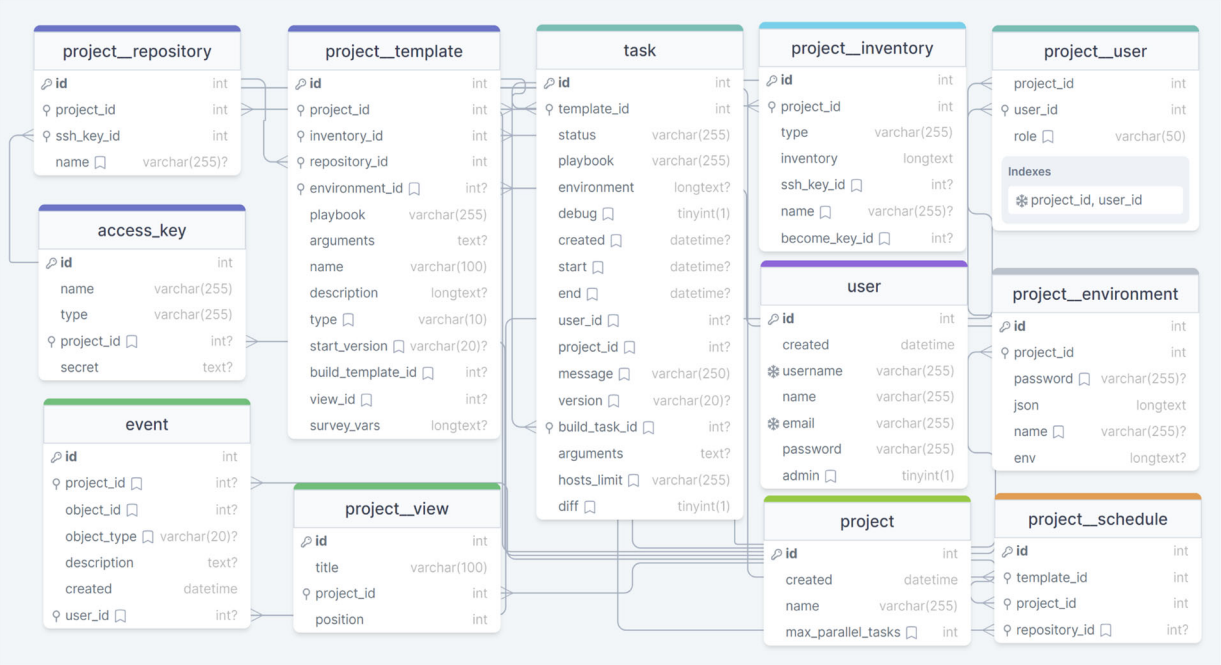

Рис. 1. ER-диаграмма базы данных

Таблица project__inventory: содержит информацию об инвентарях проекта, которые могут использоваться для определения набора узлов в задачах. Связана с таблицей project через поле project_id.

Каждая из этих таблиц связана с другими таблицами через внешние ключи, что обеспечивает целостность данных и эффективную организацию информации о проектах и задачах.

Далее представлена ER-диаграмма базы данных (рис. 1), которая визуализирует связи между таблицами и основные сущности системы управления проектами и задачами.

Имея представление о структуре базы данных и основных компонентах системы, перейдем к процессу установки, конфигурирования и работы с этой системой (рис. 2).

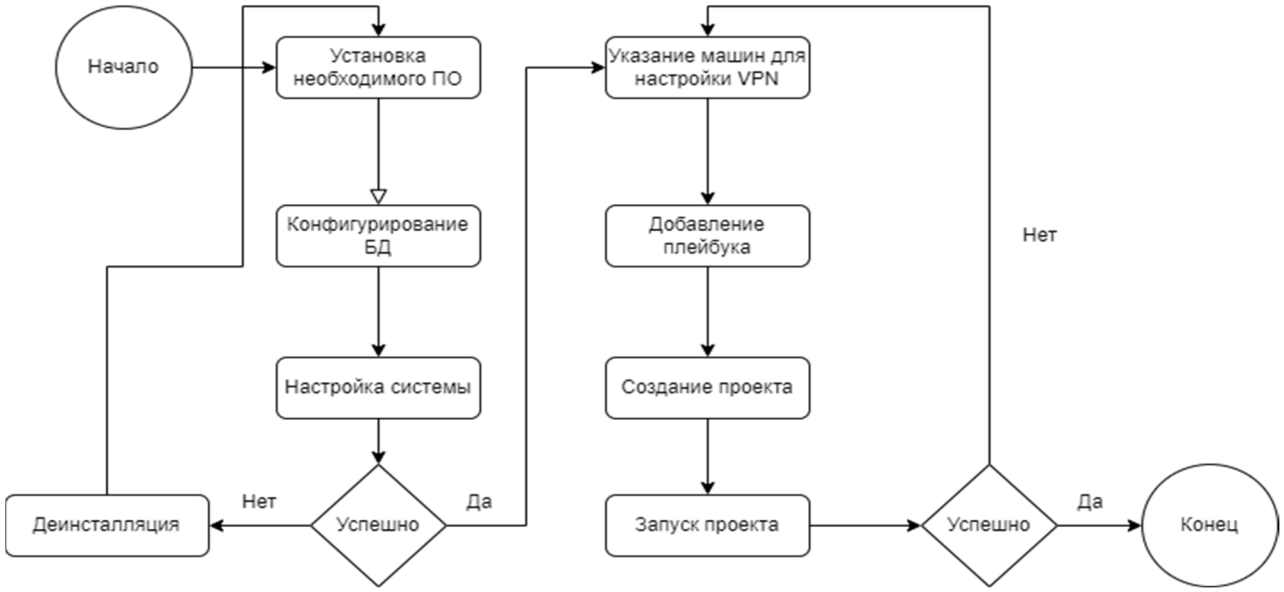

Рис. 2. Блок-схема алгоритма настройки и запуска системы

На данной блок-схеме показана блок-схема алгоритма установки языка программирования Go, базы данных MySQL и Ansible, создание базы данных. Настройка системы включает в себя следующие шаги: подключение инструмента к базе данных, выбор порта, где будет работать инструмент. Далее производится настройка подключения хостовой машины к нодам, выбор плейбука, создание и запуск проекта.

Заключение

Система автоматизированной настройки виртуальных защищенных каналов связи представляет собой важное направление развития в области сетевой безопасности. Автоматизация процесса настройки и управления защищенными каналами связи позволяет организациям эффективно реагировать на угрозы и минимизировать риски безопасности.

Развитие и внедрение системы автоматизированной настройки виртуальных защищенных каналов связи является ключевым шагом в обеспечении надежной защиты информации и инфраструктуры организации. Это позволит повысить уровень безопасности сетей, снизить вероятность кибератак и минимизировать риски для бизнеса. В будущем с развитием технологий и усовершенствованием методов автоматизации система виртуальных защищенных каналов связи будет играть все более важную роль в обеспечении кибербезопасности в условиях быстро меняющейся среды.

В данной работе была спроектирована и разработана система автоматизированной настройки виртуальных защищенных каналов связи. Главным итогом работы является собственная программная реализация данной системы.

В ходе работы были получены следующие результаты:

– исследована предметная область;

– выбран технологический стек;
– разработана программная реализация предложенного решения (MVP).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Отчет Jet Security Team // Инфосистемы Джет. – URL: https://jetcsirt.su/upload/godovoy_otchet__jet_2023.pdf.

2. Khramov I. Y. et al. Automation of VPN Tunnel Deployment between Trusted Users //2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). – IEEE, 2021. – С. 449-453.

3. Bringhenti D. et al. Automation for network security configuration: State of the art and research Trends //ACM Computing Surveys. – 2023. – Т. 56. – №. 3. – С. 1-37.

4. Басыня, Е. А. Комплексная методология интеллектуально-адаптивного управления информационной инфраструктурой предприятия / Е. А. Басыня // Защита информации. Инсайд. – 2021. – № 5(101). – С. 16-25.

5. Басыня, Е. А. Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации / Е. А. Басыня, В. Е. Хиценко, А. А. Рудковский // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2019. – Т. 22, № 2. – С. 45-51.

6. Басыня Е. А. Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия //Безопасность информационных технологий. – 2018. – Т. 25. – №. 4. – С. 42-51.

7. Xu Z., Ni J. Research on network security of VPN technology //2020 International Conference on Information Science and Education (ICISE-IE). – IEEE, 2020. – С. 539-542.

8. Pudelko M. et al. Performance analysis of VPN gateways //2020 IFIP Networking Conference (Networking). – IEEE, 2020. – С. 325-333.

9. Goel A. et al. Detection of VPN Network Traffic //2022 IEEE Delhi Section Conference (DELCON). – IEEE, 2022. – С. 1-9.

10. Tanadechopon T., Kasemsontitum B. Performance Evaluation of Programming Languages as API Services for Cloud Environments: A Comparative Study of PHP, Python, Node. js and Golang //2023 7th International Conference on Information Technology (InCIT). – IEEE, 2023. – С. 293-297.

11. Marchuk Y., Dyyak I., Makar I. Performance Analysis of Database Access: Comparison of Direct Connection, ORM, REST API and GraphQL Approaches //2023 IEEE 13th International Conference on Electronics and Information Technologies (ELIT). – IEEE, 2023. – С. 174-176.

12. Gao P. et al. Research on Performance Optimization of MySQL Database //2023 IEEE 3rd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA). – IEEE, 2023. – Т. 3. – С. 869-872.

13. Freeman J., Keating J. Mastering Ansible: Automate configuration management and overcome deployment challenges with Ansible. – Packt Publishing Ltd, 2021.

14. Aung S. T., Thein T. Comparative analysis of site-to-site layer 2 virtual private networks //2020 IEEE Conference on Computer Applications (ICCA). – IEEE, 2020. – С. 1-5.

15. Lipp B., Blanchet B., Bhargavan K. A mechanised cryptographic proof of the WireGuard virtual private network protocol //2019 IEEE European Symposium on Security and Privacy (EuroS&P). – IEEE, 2019. – С. 231-246.