УДК 004.056.5

А. А. Колпакова[1], М. Ф. Эйхман[1,2]*

Система безопасного удаленного доступа к операционным системам семействам Linux

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
[2] Научно-исследовательский институт информационно-коммуникационных технологий, г. Москва, Российская Федерация
* e-mail: akolpakovaa@mail.ru

Аннотация. В статье рассмотрена реализация системы удаленного сетевого доступа, обеспечивающей конфиденциальность и анонимность процесса удаленного подключения. Конфиденциальность обеспечивается модифицированной технологией «простукивания портов», а анонимность – технологией луковой маршрутизации. Модификация технологии заключается в динамической генерации последовательности портов с помощью аппарата нечеткой логики. Такая система устойчива к средствам сканирования и зондирования сети, а также в отличие от существующих решений обеспечивает доступность канала связи за счет использования средства контейнеризации *Docker* в совокупности с использованием балансировщика нагрузки *HAProxy*. 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, tcp/ip, port knocking, tor, балансировка нагрузки

A. A. Kolpakova[1], M. F. Eykhman[1,2]*

System of Secure Remote Access to Operating Systems of Linux Families

[1] National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russian Federation
[2] Institute of Information and Communication Technologies, Moscow, Russian Federation
* e-mail: akolpakovaa@mail.ru

Abstract. This article gives the implementation of a remote network access system that provides confidentiality and anonymity of the remote connection process. Confidentiality is provided by the modified technology of "port knocking", and anonymity is provided by the technology of onion routing. The modification of the technology consists in dynamic sequence generation by fuzzy logic algorithms. A system is resistant to scanning and probing of the network, and unlike existing solutions provides availability of the communication channel due to the use of containerization tool Docker in conjunction with load balancing HAProxy. The field of application of the tool is ensuring network information security of corporate computer networks, in particular, network end nodes under the control of operating systems of the Linux family, operating on the basis of TCP/IP protocol stack.

Keywords: remote access, tcp/ip, port knocking, tor, load balancing

Введение

Развитие информационно-коммуникационных технологий сопровождается увеличением количества атак, направленных на различные сферы в этой области. Помимо эксплуатации уязвимостей в программном обеспечении, атаки также направлены на компрометацию методов, технологий и протоколов, используемых в сфере информационных технологий. Стек протоколов *TCP/IP* также подвержен уязвимостям, включая те, которые связаны с протоколами удаленного доступа.

Термин «удаленный доступ» охватывает широкий спектр типов и сценариев взаимодействия между компьютерами, сетями и приложениями. Такое взаимодействие в стеке протоколов *TCP/IP* осуществляется с использованием различных протоколов, таких как *Telnet*, *SSH* (от англ. *Secure Shell*), *RDP* (от англ. *Remote Desktop Protocol*). Каждый из этих протоколов имеет свои уязвимости, которые могут быть использованы злоумышленниками для получения несанкционированного доступа к узлу в корпоративной сети, что способствует распространению атак в различных направлениях.

Например, протокол *Telnet* осуществляет передачу всех данных, включая пароли, без использования шифрования. Уязвимости протокола *SSH* связаны с механизмами шифрования, поддерживаемыми этим протоколом, что может привести к возможному раскрытию конфиденциальной информации. Проприетарный протокол *RDP* также имеет ряд уязвимостей, таких как *BlueKeep*, *CVE-2020-16927* (отказ в обслуживании), *CVE-2022-22015* (раскрытие информации), *CVE-2020-0610* (удаленное выполнение кода), а также другие.

Одной из популярных технологий, предназначенных для обеспечения конфиденциальности, является технология «простукивания портов» (англ. *Port Knocking*). Классическая реализация этой технологии уязвима перед средствами сканирования и зондирования сети, что может позволить злоумышленнику воспроизвести предопределенную последовательность портов и получить доступ к удаленному серверу.

Существуют усовершенствованные варианты реализации технологии *Port Knocking*, направленные на предотвращение возможности воспроизведения определенной последовательности портов. Эти варианты включают в себя отправку специально сформированного единичного пакета и разнообразные методы конфигурации динамической последовательности. Изменение порядка портов при каждом новом подключении предъявляет к реализации этой технологии следующие требования: необходимость синхронизации между сервером и клиентом, а также разработку эффективного алгоритма формирования последовательности. Этим вопросом занимаются такие исследователи, как *Pali I., Amin R., Zidan A., Amin K. M., Junquera-Sanchez J., Shiraz M.*, *Andreatos A. S.* и многие другие [1–8].

Еще одним значимым подходом является применение оверлейных технологий с целью обеспечения анонимности в процессе удаленного сетевого взаимо-

действия. В этой области исследования ведутся научной школой «Сетевая информационная безопасность» под руководством Басыни Е.А. [9–11].

Таким образом, возрастает актуальность разработки решений, обеспечивающих информационную безопасность процесса удаленного сетевого взаимодействия в условиях наличия глобального наблюдателя.

Постановка задачи

Целью настоящей работы является обеспечение конфиденциальности и анонимности процесса удаленного сетевого доступа в операционных системах семейства *Linux*.

В ходе работы была проведена ее декомпозиция на следующие задачи:

1) исследование предметной области;
2) проектирование системы безопасного удаленного доступа;
3) программная реализация предложенного решения;
4) проведение автоматизированного тестирования.

Предлагаемое решение

Проектирование системы безопасного удаленного доступа требует использования передовых методов обеспечения конфиденциальности и безопасности в сетевом взаимодействии. Разработанная система основана на модификации технологии *Port Knocking* и использовании оверлейной технологии *Tor*, предназначенной для анонимизации сетевого трафика.

Ключевыми компонентами реализованной системы удаленного сетевого взаимодействия (рис. 1) являются серверная часть, *docker*-контейнеры для инкапсуляции трафика в сеть *Tor*, сервер для балансировки нагрузки между контейнерами, а также клиентская часть.

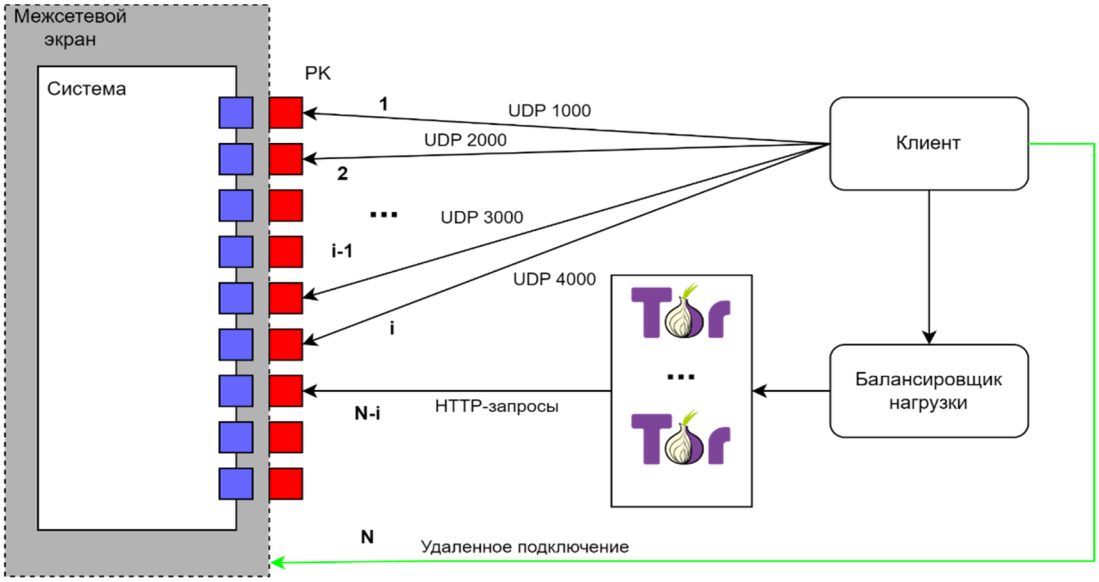

Рис. 1. Структурная схема системы удаленного сетевого доступа

Работу системы безопасного удаленного доступа обеспечивают три разработанных алгоритма: алгоритм генерации последовательности, алгоритм выбора данных блоком нечеткой логики и алгоритм работы сервера.

Алгоритм генерации последовательности портов (рис. 2) использует разные источники информации. В первую очередь, он основывается на анализе предыдущих сеансов подключения, включая такие параметры, как количество переданных пакетов, а также информацию о временных метках подключений. Эти данные подвергаются обработке с использованием блока нечеткой логики, что позволяет формировать различные последовательности в разных условиях сетевого окружения. В данной работе под термином «нечеткая логика» подразумевается множество вложенных конструкций *if-else*. Кроме того, в алгоритме учитывается текущая дата, которая служит дополнительным фактором для формирования последовательности портов. Наконец, в процессе генерации также участвуют случайно сгенерированные параметры, что усложняет прогнозирование последовательностей при новых подключениях.

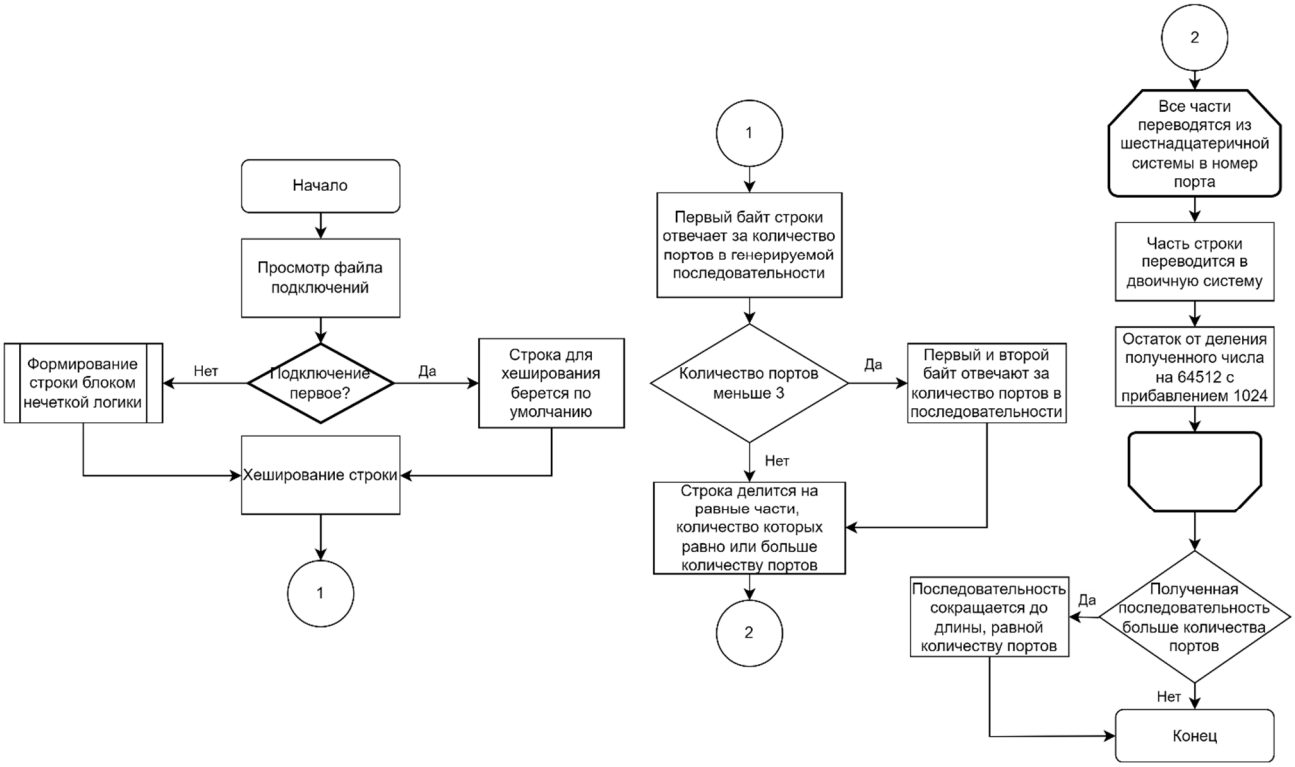

Рис. 2. Блок-схема алгоритма генерации последовательности портов

Блок нечеткой логики (рис. 3) представляет собой базу правил вида *IF <утверждение> THEN <результат>*, на основе которых будет формироваться нечеткий вывод. Отобранные параметры подключения для утверждений включают количество пакетов, дату и время подключения. Выбранные параметры сравниваются с количеством пакетов при предыдущем подключении, а также с текущими временем и датой.

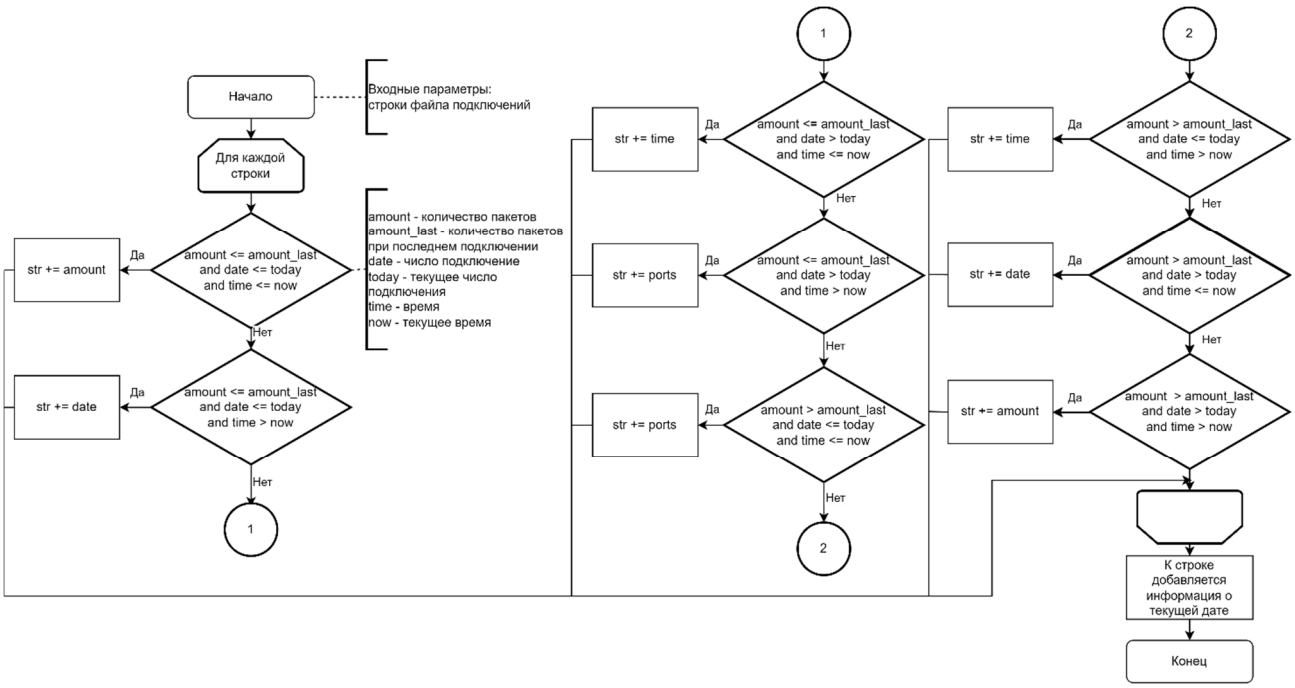

Рис. 3. Блок-схема алгоритма выбора данных блоком нечеткой логики

Поскольку ранее приводились лишь алгоритмы отдельных процессов системы удаленного сетевого взаимодействия, то для демонстрации работы необходимо привести *UML*-моделирование проектируемой системы (рис. 4).

Существует большое количество различных типов *UML*-диаграмм, охватывающих широкий спектр аспектов моделирования систем, начиная от диаграммы классов и заканчивая диаграммой синхронизации. Работа проектируемой системы удаленного доступа сильно связана со временем, поэтому для иллюстрации функционирования всей системы лучше всего подойдет диаграмма последовательности.

Диаграмма последовательности позволяет продемонстрировать все взаимодействующие объекты системы, а также показать их появление во времени при работе системы. Также на такой диаграмме наглядно видно, какими сообщениями и когда обмениваются все объекты взаимодействия.

Процесс установления соединения начинается с генерации последовательности портов клиентом и сервером. После завершения этого этапа клиент отправляет пакеты на сервер согласно сгенерированной последовательности. На сервере происходит проверка пришедших пакетов на правильность и соответствие сформированной последовательности. После отправки последовательности пакетов клиент запускает процесс отправки *HTTPS* запросов через сеть *Tor*. Эти запросы способствуют установлению анонимности и сокрытию идентифицирующей информации о клиенте. По завершении этого этапа клиент получает доступ к удаленному подключению, что предоставляет возможность безопасного и защищенного удаленного взаимодействия между клиентом и сервером.

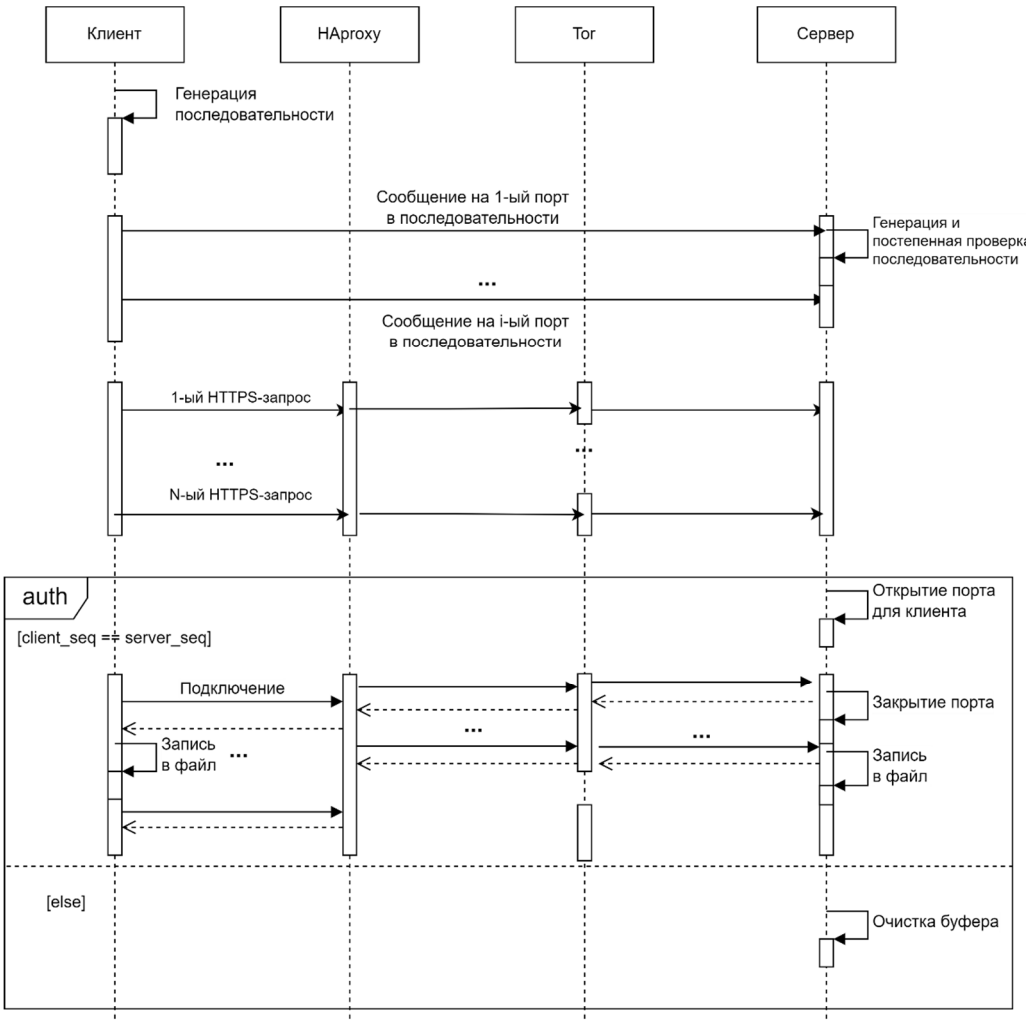

Рис. 4. *UML*-диаграмма последовательности работы системы

Дальнейшее удаленное взаимодействие становится возможным благодаря применению технологии *VPN*. В данной системе выбор пал на *OpenVPN* для обеспечения безопасного и защищенного соединения между клиентом и сервером.

Тестирование

В данной работе для демонстрации работоспособности и корректности предложенного решения проводился статический анализ кода, модульное тестирование, а также ручное тестирование.

Модульное тестирование позволяет осуществить проверку отдельных модулей программного обеспечения с целью выявления и исправления потенциальных дефектов и ошибок в их функционировании. В данной работе модульные тесты, использующие фреймворк *unittest* [12], направлены на проверку точности и правильности работы алгоритмов формирования последовательности портов, а также на анализ корректности обработки входящих пакетов данных, что является критически важным аспектом для обеспечения надежности и безопасности функционирования системы удаленного доступа.

Ручное тестирование заключалось в проверке определения состояния порта с помощью утилиты *Nmap* [13]. Данный вид тестирования позволил определить, что поведение разработанной системы соответствует аналогичным решениям, основанных на технологии *Port Knocking*, таким как *knockd* [14] и *fwknock* [15].

Заключение

В рамках данной работы была предложена система удаленного сетевого доступа с обеспечением конфиденциальности и анонимности данного процесса, которая была программно реализована и успешно протестирована.

Теоретическая значимость работы заключается в проектировании алгоритмов, 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. 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.

2. 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.

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

4. Shiraz M. et al. An improved port knocking authentication framework for mobile cloud computing //Malaysian Journal of Computer Science. – 2019. – Т. 32. – №. 4. – С. 269-283.

5. Andreatos A. S. Hiding the SSH port via smart Port Knocking //International Journal of Computers. – 2017. – Т. 11. – С. 28-31.

6. Vardeva I. Intuitionistic Fuzzy Estimations of Implementation of Port Knocking on Routeros //2022 8th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE). – IEEE, 2022. – С. 1-4

7. Fang W., Guan X. Research on iOS remote security access technology based on zero trust //2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC). – IEEE, 2022. – Т. 6. – С. 238-241.

8. Nugroho M. A. et al. Port Knocking Implementation on Programmable Data Plane //2021 13th International Conference on Information & Communication Technology and System (ICTS). – IEEE, 2021. – С. 35-39.

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 multi-layer encryption and overlay technologies / E. A. Basinya, Z. B. Akhayeva, D. H. Omarkhanova, G. B. Tolegenova [et al.] // 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. Unit testing framework. – URL: https://docs.python.org/3/library/unittest.html (дата обращения: 21.04.2024).

13. Nmap. – URL: https://nmap.org/ (дата обращения: 21.04.2024).

14. knockd. – URL: https://linux.die.net/man/1/knockd (дата обращения: 21.04.2024).

15. fwknop. – URL: https://github.com/mrash/fwknop (дата обращения: 21.04.2024).

© А. А. Колпакова, М. Ф. Эйхман, 2024