УДК 004.057.4

*А. А. Колпакова*[1]*

# Обзор технологий удаленного сетевого доступа

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

**Аннотация.** В статье представлен обзор протоколов удаленного доступа. Выделены преимущества и недостатки каждого из протоколов, а также уязвимости, связанные с ними. Описывается один из возможных способов обеспечения сетевой информационной безопасности, базирующийся на виртуальных защищенных каналах связи. Приведены основные протоколы VPN, включая L2TP/IPSec, OpenVPN и WireGuard, и описаны их преимущества и недостатки. Рассмотрен ряд важных факторов при выборе протокола VPN, таких как уровень безопасности, скорость и доступность. Выделены некоторые способы обеспечения конфиденциальности и анонимности процесса удаленного сетевого взаимодействия. Приведенное исследование предметной области может использоваться для проектирования и конфигурирования решений по безопасному и эффективному удаленному доступу к сетевым ресурсам посредством комбинирования различных технологий.

**Ключевые слова:** удаленный доступ, SSH, RDP, Telnet, VPN, Port Knocking

*A. A. Kolpakova*[1]*

# An overview of remote network access technologies

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

**Abstract.** This article gives an overview of remote access protocols. The advantages and disadvantages of each protocol, as well as the vulnerabilities associated with them, are highlighted. It describes one of the possible ways to ensure network information security based on virtual secure communication channels. The main VPN protocols, including L2TP/IPSec, OpenVPN and WireGuard, and their advantages and disadvantages are described. A number of important factors in choosing a VPN protocol are discussed, such as security, speed, and availability. Some ways to ensure confidentiality and anonymity of the remote network communication process are highlighted. This case study can be used to design and configure solutions for secure and efficient remote access to network resources by combining different technologies.

**Keywords:** remote access, SSH, RDP, Telnet, VPN, Port Knocking

## *Введение*

Развитие информационно-коммуникационных технологий приводит к росту атак на различные области этой сферы. Помимо эксплуатации уязвимостей в различном программном обеспечении атаки производятся также на методы, технологии, протоколы, на которых основана работа программного обеспечения (ПО). Так, стек протоколов TCP/IP (англ. Transmission Control Protocol/Internet Protocol) имеет свои уязвимости, связанные в том числе с протоколами удаленного доступа.

Под словосочетанием «удаленный доступ» скрывается широкое понятие, включающее в себя различные типы и варианты взаимодействия компьютеров, сетей и приложений. Осуществление такого взаимодействия в стеке протоколов TCP/IP могут обеспечивать следующие протоколы:

– протокол эмуляции терминала (англ. Telnet);

– протокол безопасной оболочки (англ. Secure Shell, SSH);

– протокол удаленного рабочего стола (англ. Remote Desktop Protocol, RDP).

Согласно данным поисковой системы Shodan, в мире около 34 млн. устройств, использующих ранее упомянутые протоколы [1]. В этой статистике используются только те устройства, в которых явно открыт порт, используемый протоколом по умолчанию.

Ведущие вендоры сферы информационной безопасности постоянно выкладывают отчеты по статистикам атак и прогнозам на ближайшее время. Согласно статье компании ESET, удаленная и гибридная работы находятся среди 10 проблем информационной безопасности [2]. Другая статистика от «Лаборатории Касперского» говорит о том, что Россия вошла в пятерку стран, в которых их решения заблокировали наибольшее число попыток атак на малый и средний бизнес через протоколы удаленного доступа (RDP) в январе-апреле 2022 года — почти 27,5 миллионов [3].

Таким образом, актуальность данной статьи обусловлена увеличением количества устройств, использующих протоколы удаленного сетевого доступа, а также с возрастанием количества атак на эти протоколы, поскольку получение доступа к одному устройству корпоративной вычислительной сети может привести к компрометации конфиденциальных данных, ущербу компании и инфраструктуре предприятия.

### *Постановка задачи*

Целью настоящей работы является исследование предметной области, которое включает в себя обзор протоколов удаленного сетевого доступа, технологии VPN, а также анализ существующих научных работ, посвященных обеспечению информационной безопасности процесса удаленного сетевого взаимодействия.

### *Обзор*

Одним из первых протоколов удаленного администрирования является протокол Telnet, который не обеспечивает надежную защиту данных. Он использует незашифрованную передачу данных, включая пароли, поэтому все данные, передаваемые через Telnet, могут быть перехвачены и прочитаны злоумышленниками [4]. Другим недостатком протокола Telnet является отсутствие проверки подлинности данных. Это означает, что любой пользователь может подключиться к удаленному узлу с помощью Telnet, используя произвольное имя пользователя и пароль, даже если они неверны. Кроме того, Telnet уязвим к различным видам атак, таким как атаки на протокол транспортного уровня TCP, атака SYN-пакетами (англ. SYN flooding) и перехват сессии TCP (англ. TCP session

hijacking). В целом, использование протокола Telnet не рекомендуется в современных сетевых средах.

В 1995 году была создана первая версия протокола SSH для замены небезопасного протокола Telnet. В отличие от Telnet, версия SSH-1 предотвращала атаки на прослушивание трафика, но оставалась уязвимой для атак посредника (англ. Man-In-The-Middle, MITM). Устранение технических недостатков первой версии привели к созданию второй версии протокола SSH-2.

Новая версия SSH обеспечивает лучшую защиту данных за счет использования протокола обмена ключами Диффи-Хеллмана и проверки целостности сообщений с помощью кода аутентификации сообщений (англ. MAC). Спецификация протокола SSH-2 содержится в документе RFC 4251 [5]. Кроме того, вторая версия протокола устойчива к атакам на присоединение к сессии (англ. Session Hijacking).

Подключение по SSH состоит из нескольких этапов.

1. *Установление TCP-соединения*. Клиент подключается к TCP-порту сервера, который прослушивается SSH-сервером. По умолчанию используется 22 порт.

2. *Настройка защищенного канала.* Этот этап предназначен для обмена правилами взаимодействия между клиентом и сервером для согласования алгоритмов работы, обмена идентификационными данными, а также для генерации сессионного ключа.

3. *Аутентификация.* Протокол SSH поддерживает три варианта аутентификации: по паролю, по ключам и по IP. Аутентификация по паролю является наиболее распространенной, но для повышения безопасности необходимо использовать аутентификацию по ключам, потому что при таком подходе ничего не передается. Сервер проверяет, что клиент владеет не только открытым, но и закрытым ключом. Аутентификация по IP является совершенно небезопасной, поскольку простая подмена IP-адреса позволяет получить доступ к серверу, поэтому такая возможность чаще отключена.

Во второй версии протокола SSH используется слепок ключа для предотвращения атак типа MITM, позволяющий проверить соответствие ключа сервера на стороне клиента. Тем не менее, возможны атаки MITM, которые могут изменять слепок ключа сервера в файле «известных хостов», что позволяет злоумышленнику перехватить сессию клиента. Первым этапом является атака подмены ARP (англ. ARP-spoofing) для обнаружения установленных сессий, а затем на следующем этапе злоумышленник дожидается нового подключения и перехватывает сессию в момент подключения. Кроме того, уязвимости протокола SSH связаны с режимами шифрования, поддерживаемыми протоколом. Это может привести к возможности восстановления зашифрованных данных.

Протокол RDP в отличии от двух упомянутых ранее протоколов является проприетарным протоколом удаленного сетевого взаимодействия от компании Microsoft. Аналогично Telnet и SSH, используется клиент-серверная модель взаимодействия, но в отличие от предыдущих протоколов пользователю предоставляется графический интерфейс для управления устройством.

Проблемой любого проприетарного программного обеспечения является большой промежуток времени между обнаружением уязвимости и выходом обновления, исправляющего эту уязвимость. Протокол RDP не является исключением.

Одна из известных критических уязвимостей, связанная с реализацией протокола, называется BlueKeep, или CVE-2019-0708 [6]. Эта уязвимость затрагивает устройства начиная с Windows 2000 и заканчивая Windows Server 2008 R2 и Windows 7. В реализации протокола RDP используется множество виртуальных каналов для передачи различных видов данных. При создании сессии создается 32 статических канала, к которым могут привязываться или удаляться динамические каналы, созданные по запросу клиента. По умолчанию 31 канал резервируется RDP для внутреннего использования и имеет название «MS_T120». Поскольку проверки имени виртуального канала, созданного пользователем, не осуществляется, то злоумышленник может создать канал с таким же именем и привязать к другому статическому каналу. При этом с новым номером будет связан указатель на существующий экземпляр динамического канала «MS_T120». При закрытии созданного злоумышленником канала происходит освобождение памяти, после чего в системе остаётся связанный с номером 31 висячий указатель на канал «MS_T120», что может приводить к ошибкам доступа к памяти. Исправленная версия драйвера termdd.sys не позволяет назначать каналу с названием «MS_T120» номера, отличные от 31.

Таким образом, использование рассмотренных протоколов в стандартном виде недопустимо. Обеспечение минимальной безопасности заключается в использовании новых версий протоколов, изменении дефолтных портов, ограничении количества неправильных попыток ввода паролей, повышении уровня шифрования и т.д. Безопасным решением является использование таких протоколов внутри защищенного канала связи с помощью технологии VPN (англ. Virtual Private Network). Известными реализациями данной технологии являются протоколы IPsec (англ. Internet Protocol Security), OpenVPN и Wireguard.

Функционирование IPSec может происходить в двух режимах: туннельном и транспортном. При работе в туннельном режиме весь IP-пакет подвергается шифрованию, в то время как в транспортном режиме шифрованию подвергается только содержимое пакета. Кроме того, соединение между узлами может быть установлено через другие технологии, такие как L2TP (англ. Layer 2 Tunnel Protocol) или другие.

Протокол IPSec включает в себя AH (англ. Authentication Header) и ESP (англ. Encapsulating Security Payload). AH обеспечивает целостность данных, аутентификацию и функцию предотвращения повторной передачи пакетов, а ESP шифрует передаваемую информацию и ограничивает поток конфиденциального трафика [7].

Другой реализацией технологии VPN является OpenVPN, реализация с открытым исходным кодом, которая позволяет создавать зашифрованные каналы связи между устройствами в сети [8]. OpenVPN в отличие от IPsec использует библиотеку OpenSSL для обеспечения безопасности данных. Целостность пере-

даваемых данных по каналу связи в OpenVPN обеспечивается за счет механизма HMAC (англ. Hash-based Message Authentication Code) в сочетании с алгоритмами хэширования. Кроме того, OpenVPN позволяет использовать как предустановленные ключи, так и сертификаты X.509 – формат сертификатов открытых ключей, стандартизированный организацией ITU-T.

Одной из последних реализаций технологии VPN является протокол WireGuard, который предназначен для защиты соединений между устройствами в глобальной вычислительной сети Интернет. Он был разработан в 2016 году и отличается высокой скоростью, простотой использования и безопасностью. Стоит отметить, что WireGuard использует только UDP [9].

В WireGuard применяется симметричное шифрование, что уменьшает вычислительную нагрузку и улучшает производительность. Он также использует асимметричные ключи для установления безопасного канала связи, а затем – симметричное шифрование для шифрования трафика. Это делает WireGuard более быстрым и производительным, чем традиционные VPN-протоколы, такие как OpenVPN и IPSec.

Протокол WireGuard также поддерживает IPv6 и обеспечивает целостность данных, защиту от атак повторного воспроизведения (англ. Replay Attack) и атак типа «отказ в обслуживании» (англ. Denial of Service, DoS).

Несмотря на разные методы защиты, используемые различными реализациями технологии VPN, в них часто находят большой спектр уязвимостей. К примеру, обнаруживают такие уязвимости, как:

– CVE-2022-33738 [10]: использование слабого генератора случайных чисел в OpenVPN для создания токена сеанса пользователя для веб-портала;

– CVE-2022-27666 [11]: в коде преобразования IPSec ESP в файле esp4.c для IPv4 и esp6.c для IPv6 была обнаружена ошибка переполнения буфера кучи. Эта ошибка может позволить локальному злоумышленнику с обычными пользовательскими привилегиями изменять объекты в куче ядра, что представляет угрозу повышения локальных привилегий;

– CVE-2021-46873 [12]: WireGuard, например, версия 0.5.3 для Windows, не полностью учитывает возможность того, что злоумышленник сможет установить системное время у жертвы на будущее значение, например, из-за использования не аутентифицированного сервера NTP (англ. Network Time Protocol). Это может привести к результату, при котором один статический закрытый ключ становится бесполезным.

Одной из важнейших задач конфигурирования сетевого оборудования является организация удаленного сетевого взаимодействия, поскольку такие единицы сети, как, например, межсетевой экран, отвечают за обеспечение безопасности большей части корпоративной вычислительной сети. Во многих реализациях используются протоколы удаленного доступа стека TCP/IP. В связи с этим следует обеспечить те методы защиты, которые позволят закрыть уязвимости в реализации этих протоколов, а также привнести новые слои безопасности.

Одной из популярных технологий, используемой для обеспечения конфиденциальности процесса удаленного сетевого взаимодействия, является технология «простукивания портов» (англ. Port Knocking). Работа Port Knocking в классической реализации происходит следующим образом: на сервере задается конечная последовательность портов, на которые клиент должен отправить пакеты, чтобы в дальнейшем получить доступ к закрытому порту сервера. Работа базовой реализации продемонстрирована на рис. 1.

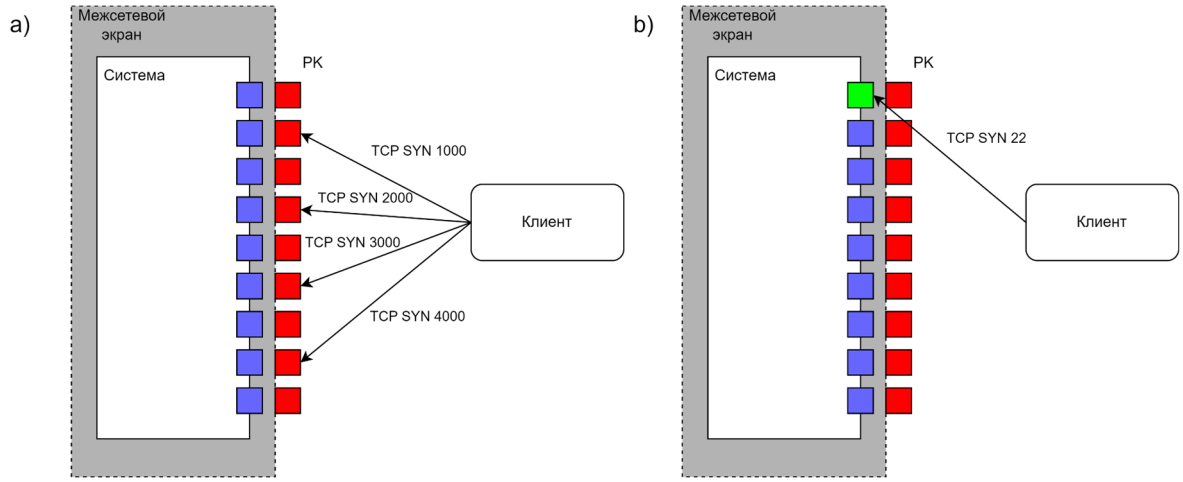


Рис. 1. Работа технологии Port Knocking: a) отправка последовательности клиентом; b) открытие порта межсетевым экраном сервера и подключение клиента

Можно заметить, что при статичной последовательности рассматриваемая технология уязвима перед средствами сканирования и зондирования сети, что позволяет злоумышленнику воспроизвести заданную последовательность и получить доступ к закрытому порту.

Существуют расширенные реализации технологии «простукивания портов» для предотвращения воспроизведения последовательности, начиная с отправки правильно сконфигурированного единственного пакета и заканчивая различными реализациями конфигурирования динамической последовательности. Изменяющаяся с каждым подключением очередность портов ставит при реализации две задачи: процесс синхронизации сервера и клиента и алгоритм формирования последовательности. Этим занимается ряд ученых Pali I., Amin R., Zidan A., Amin K. M., Junquera-Sanchez J., Shiraz M. и Andreatos A. S. [13-17]. Другим интересным решением является использование оверлейных технологий и многослойного шифрования для обеспечения информационной безопасности процесса удаленного сетевого взаимодействия. В рамках научных изысканий данным направлением занимается научная школа Басыни Е.А. [18-20].

Стоит отметить, что при грамотном выборе технологий удаленного сетевого доступа, а также их правильной настройке возможно достичь высокого уровня информационной безопасности.

## *Заключение*

В рамках статьи был проведен обзор технологий удаленного сетевого взаимодействия, а также рассмотрены их различные уязвимости. Протоколы удаленного доступа стека протоколов TCP/IP не обеспечивают необходимый уровень информационной безопасности. Причины этого заключаются в их недостаточной стойкости к различного видам атак: атакам посредника, перехвата сессии и многим другим. Тем не менее существует возможность создать безопасное удаленное соединение с помощью совокупности технологий виртуальных защищенных каналов связи, технологий обеспечения конфиденциальности информационных потоков, а также оверлейных технологий.

Значимость работы заключается в том, что результаты проведенного исследования могут в дальнейшем использоваться для проектирования и реализации собственных решений по организации безопасного и эффективного удаленного сетевого доступа.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Shodan [Электронный ресурс]. — URL: https://www.shodan.io/ (дата обращения: 26.04.2023).
2. The future starts now: 10 major challenges facing cybersecurity [Электронный ресурс]. — URL: https://www.welivesecurity.com/2022/11/03/future-starts-10-major-challenges-facing-cybersecurity/ (дата обращения: 26.04.2023).
3. Лаборатория Касперского [Электронный ресурс]. — URL: https://www.kaspersky.ru/about/press-releases/2022_laboratoriya-kasperskogo-v-rossii-bolee-chem-v-15-raza-vyroslo-chislo-popytok-ukrast-paroli-nebolshih-kompanij (дата обращения: 26.04.2023).
4. Карпенко, М. Исследование передачи трафика данных в защищенном и открытом доступе / М. Карпенко, П. Дунаев // Journal of Science. Lyon. — 2021. — No 18. — С. 38-42.
5. RFC 4251: The Secure Shell (SSH) Protocol Architecture [Электронный ресурс]. — URL: https://www.rfc-editor.org/rfc/rfc4251 (дата обращения: 26.04.2023)
6. CVE-2019-0708 Detail [Электронный ресурс]. — URL: https://nvd.nist.gov/vuln/detail/CVE-2019-0708 (дата обращения: 26.04.2023).
7. IPSec Overview [Электронный ресурс]. — URL: https://www.ciscopress.com/articles/article.asp?p=25470 (дата обращения: 26.04.2023).
8. OpenVPN [Электронный ресурс]. — URL: https://openvpn.net/ (дата обращения: 26.04.2023).
9. WireGuard [Электронный ресурс]. — URL: https://www.wireguard.com/ (дата обращения: 26.04.2023).
10. CVE-2022-33738 Detail [Электронный ресурс]. — URL: https://nvd.nist.gov/vuln/detail/CVE-2022-33738 (дата обращения: 26.04.2023).
11. CVE-2022-27666 Detail [Электронный ресурс]. — URL: https://nvd.nist.gov/vuln/detail/CVE-2022-27666 (дата обращения: 26.04.2023).
12. CVE-2021-46873 Detail [Электронный ресурс]. — URL: https://nvd.nist.gov/vuln/detail/CVE-2021-46873 (дата обращения: 26.04.2023).
13. 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.
14. 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.

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

16. 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.

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

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

19. 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.]. – Text : direct // Journal of Theoretical and Applied Information Technology. - 2022. – Vol. 100, iss. 16. – P. 4918-4927.

20. Басыня Е. А. Программная реализация и исследование системы интеллектуально-адаптивного управления информационной инфраструктурой предприятия = Software implementation and research of the system for intellectually adaptive management of the enterprise information infrastructure / Е. А. Басыня // Вестник Самарского государственного технического университета. Серия: Технические науки = Vestnik of Camara state techmical university. Technical sciences series. - 2020. - Т. 28, № 1 (65). - С. 6-21.