ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056.5

DOI: 10.21822/2073-6185-2024-51-3-110-116 Оригинальная статья /Original article

Исследование способов повышения безопасности корпоративных сетей

Н.Ф. Махмутова, Э.В. Бирих, Д.В. Сахаров, А.С. Кривец, М.А. Дегтярев
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
193232, г. Санкт-Петербург, пр. Большевиков 22, Россия

Резюме. Цель. В статье представлены результаты исследования способа повышения безопасности корпоративной сети путем использования техники подмены адресов отправителя при пересылке пакетов между компьютерами. **Метод.** В процессе исследования были использованы методы анализа сетевого трафика, программирование на уровне сетевого протокола и алгоритмы обработки пакетов данных. Компьютеры в сети подключены к одному серверу, через который происходит общение. При пересылке пакетов между компьютерами сети подменяется адрес отправителя, а при приеме пакета другим компьютером пакет разбирается, и внутри него находится настоящий адрес отправителя. **Результат.** Предложенный способ позволяет эффективно защитить корпоративную сеть от атак, связанных с подделкой адресов отправителей пакетов данных. **Вывод.** Использование техники подмены адресов отправителя при передаче данных в корпоративной сети является эффективным способом повышения безопасности и защиты от внешних угроз. Дальнейшие исследования будут направлены на разработку более сложных и надежных методов защиты сетей.

Ключевые слова: информационная безопасность, беспроводные сети, проводные сети, корпоративные сети, ip-адрес

Для цитирования: Н.Ф. Махмутова, Э.В. Бирих, Д.В. Сахаров, А.С. Кривец, М.А. Дегтярев. Исследование способов повышения безопасности корпоративных сетей. Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(3):110-116. DOI:10.21822/2073-6185-2024-51-3-110 -116

Research of ways to improve the security of corporate networks

N.F. Makhmutova, E.V. Birikh, D.V. Sakharov, A.S. Krivets, M.A. Degtyarev
M.A. Bonch-Bruevich St. Petersburg State University of Telecommunications,
22 Bolshevikov Ave., St. Petersburg 193232, Russia

Abstract. Objective. The article explores a way to improve the security of a corporate network by using the technique of spoofing sender addresses when forwarding packets between computers. **Method.** Network traffic analysis methods, network protocol level programming and data packet processing algorithms are used. Computers on the network are connected to one server. When sending packets between computers in the network, the sender's address is replaced, and when a packet is received by another computer, the packet is disassembled, and the real sender's address is inside it. **Result.** The method allows for effective protection of a corporate network from attacks associated with the forgery of addresses of data packet senders. **Conclusion**. Using the sender address substitution technique when transmitting data in a corporate network is an effective way to increase security and protection from external threats. Further research is aimed at developing complex and reliable methods for protecting networks.

Keywords: information security, wireless, wired and corporate networks, ip address

For citation: N.F. Makhmutova, E.V. Birikh, D.V. Sakharov, A.S. Krivets, M.A. Degtyarev. Research of ways to improve the security of corporate networks. Herald of Daghestan State Technical University. Technical Sciences. 2024;51(3):110-116. DOI:10.21822/2073-6185-2024-51-3-110-116

Введение. В настоящее время беспроводные сети становятся все более популярными и широко используются как в домашних условиях, так и в корпоративной среде. Благодаря удобству и мобильности, которые они предоставляют, беспроводные сети стали неотъемлемой частью нашей повседневной жизни. Однако, вместе с увеличением использования беспроводных технологий возрастает и угроза для безопасности информации.

Защита корпоративных сетей становится все более важной, поскольку они содержат конфиденциальные данные, финансовую информацию и другие ценные ресурсы компании. Нарушение безопасности корпоративной сети может привести к серьезным последствиям, таким как утечка конфиденциальных данных, нарушение работы бизнес-процессов и финансовые потери. В статье обоснована актуальность проблемы защиты корпоративных сетей от атак, связанных с использованием техники подмены адресов отправителя, предложены методы и решения для обеспечения безопасности сети. Также рассмотрены примеры из практики и статистические данные, подтверждающие необходимость принятия мер по защите корпоративных сетей от подобных угроз.

Постановка задачи. Для повышения безопасности корпоративных сетей от угроз, связанных с конфигурацией сети, таких как перехват трафика и атаки на слабые места сети необходимо использовать технологию подмены адреса отправителя, чтобы общение устройств в сети выглядело хаотично.

Применение технологии подмены адреса отправителя позволяет эффективно затруднить возможность идентификации и отслеживания устройств в сети, что делает ее более защищенной от злоумышленников [1, 20]. Кроме того, использование подмены адреса отправителя способствует обеспечению конфиденциальности данных и защите приватности пользователей. Важным аспектом при внедрении этой технологии является правильная настройка системы и контроль за ее работой, чтобы избежать возможных негативных последствий и обеспечить стабильную и безопасную работу корпоративной сети [1-4].

Методы исследования. Для оценки эффективности технологии подмены адреса отправителя был проведен эксперимент в небольшой корпоративной сети. Для проведения эксперимента необходимы 5 устройств, находящихся в одной локальной сети. Одно из устройств будет выступать в качестве сервера, остальные же будут выступать в качестве клиентов, которые будут обмениваться данными. В качестве операционной системы для эксперимента была выбрана Ubuntu 22.04.

Описание предварительной настройки устройств:

1. Установить Python3: Язык программирования Python использовался для написания программ, которые будут запущены как на клиентах, так и на сервере;
2. Установить библиотеку Scapy для Python3: Библиотека Scapy используется для формирования сетевых пакетов, их модификации, обработки и отправки;
3. Установить программу Wireshark: Программа Wireshark используется для анализа сетевого трафика в реальном времени или из захваченных файлов захвата (pcap). В рамках эксперимента эта программа будет использоваться для анализа трафика, передаваемого в процессе обмена данными между клиентами;
4. Внести изменения в настройки утилиты sysctl: Утилита sysctl используется для динамической настройки параметров ядра во время работы системы.

В рамках данного эксперимента будут модифицированы сетевые настройки, отвечающие за отправку пакетов повторной передачи TCP-соединения (TCP retransmission):

sudo sysctl -w net.ipv4.tcp_retries1=0 и sudo sysctl -w net.ipv4.tcp_retries2=0

5. Внести изменения в настройки утилиты iptables: Утилита iptables используется для управления брандмауэром, для настройки правил фильтрации пакетов входящего и исходящего трафика, а также преобразования сетевых пакетов [8-10]. В рамках данного эксперимента будут блокироваться исходящие пакеты сброса TCP-соединения (TCP reset), отправляемые не с помощью Scapy:

```
sudo iptables -A OUTPUT -p tcp --tcp-flags RST RST -j DROP
sudo iptables -A OUTPUT -p tcp --sport 5000 --tcp-flags RST RST -j ACCEPT
```

6. На устройство, выступающее в роли сервера, необходимо загрузить программу server.py.

7. На устройства, выступающие в роли клиентов, необходимо загрузить программу client.py.

Эксперимент проведен в следующей последовательности:

Этап 1 – «Моделирование обмена данными между устройствами без использования механизма подмены ip-адресов».

1. На устройстве, выступающем в роли сервера, необходимо запустить программу server.py со следующими настройками: sudo server.py prod unix unsafe

Эта команда запустит программу для инициализации устройства-сервера в режиме без подмены ip-адресов для устройств с операционной системой семейства UNIX.

2. На устройстве, выступающем в роли сервера, необходимо запустить программу wireshark и выбрать интерфейс, указанный в командной строке при инициализации программы server.py, а также применить фильтр для отображения только TCP-пакетов, взаимодействующих с портом 5000 (этот порт используется программой в качестве порта, который прослушивает устройство-сервер для соединения с устройствами-клиентами): tcp && tc.port == 5000

3. На устройствах, выступающих в роли клиентов, необходимо запустить программу client.py со следующими настройками: sudo client.py prod unix unsafe. Эта команда запустит программу для инициализации устройств-клиентов в режиме без подмены ip-адресов для устройств с операционной системой семейства UNIX.

4. С любого устройства, выступающего в роли клиента, необходимо отправить текстовые данные, которые будут пересланы остальным клиентам, подключенным в данный момент к устройству-серверу.

5. Изучить захваченный с помощью программы wireshark сетевой трафик.

После описанных шагов можно завершать работу программ server.py, client.py и wireshark.

Этап 2 – «Моделирование обмена данными между устройствами с использованием механизма подмены ip-адресов».

1. На устройстве, выступающем в роли сервера, необходимо запустить программу server.py со следующими настройками, представленными на рис. 1.

sudo server.py prod unix safe

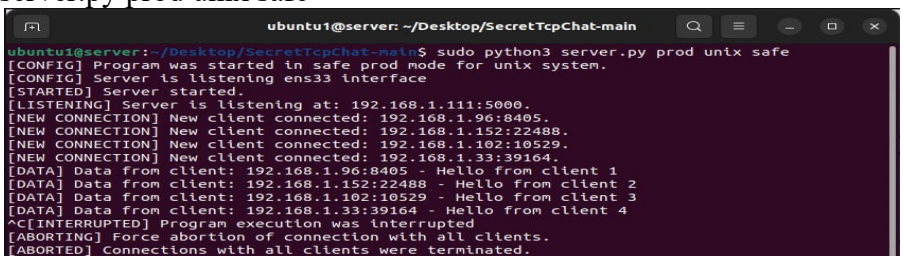

Рис. 1. Запуск сервера
Fig. 1. Starting the server

Эта команда запустит программу для инициализации устройства-сервера в режиме с подменой ip-адресов для устройств с операционной системой UNIX.

2. На устройстве, выступающем в роли сервера, необходимо запустить программу wireshark и выбрать интерфейс, указанный в командной строке при инициализации программы client.py, а также применить фильтр для отображения только TCP-пакетов, взаимодействующих с портом 5000 (этот порт используется программой в качестве порта, который прослушивает устройство-сервер для соединения с устройствами-клиентами):

tcp && tc.port == 5000

3. На устройствах, выступающих в роли клиентов, необходимо запустить программу client.py со следующими настройками, представлено на рис. 2.

sudo client.py prod unix safe

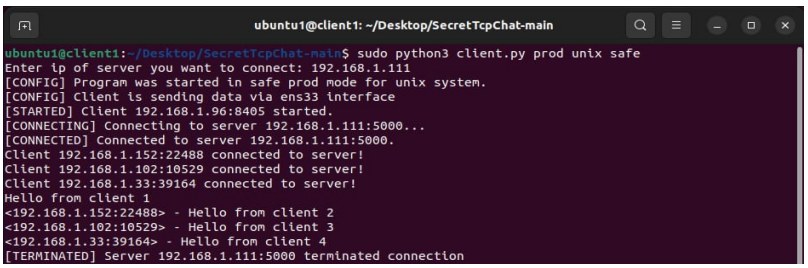

Рис. 2. Запуск клиента
Fig. 2. Starting the client

Эта команда запустит программу для инициализации устройств-клиентов в режиме с подменой ip-адресов для устройств с операционной системой UNIX. Подробное описание работы программы представлено на блок-схеме на рис. 3.

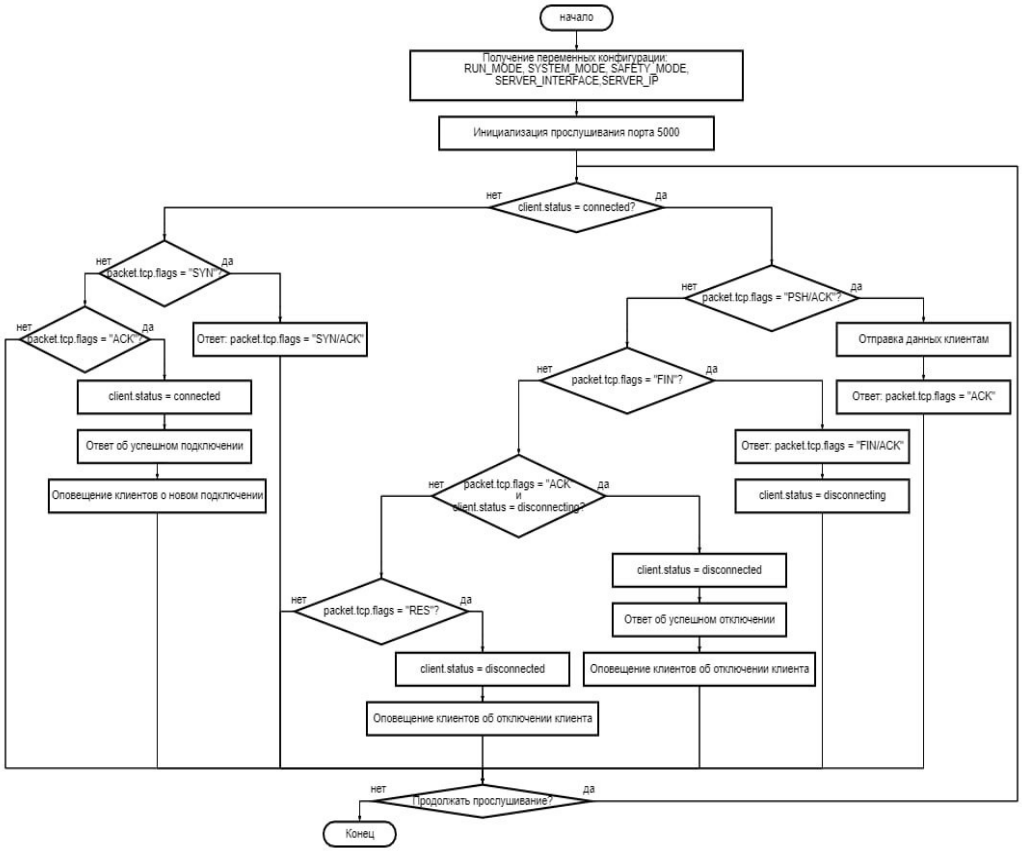

Рис. 3. Блок-схема программы
Fig. 3. The flowchart of the program

4. С любого устройства, выступающего в роли клиента, необходимо отправить текстовые данные, которые будут пересланы остальным клиентам, подключенным в данный момент к устройству-серверу [5-7].

5. Изучить захваченный с помощью программы wireshark сетевой трафик.

После описанных шагов можно завершать работу программ server.py, client.py и wireshark.

Обсуждение результатов. В результате проведенного эксперимента было установлено, что применение метода подмены адреса отправителя существенно улучшает безопасность корпоративных сетей. Этот метод затрудняет определение конфигурации сети и обнаружение её уязвимых мест, снижая вероятность успешных атак, основанных на знании конфигурации [11-14]. Рассмотрим дампы, снятые во время проведения эксперимента с использованием подмены адресов и без нее (рис. 4 и 5).

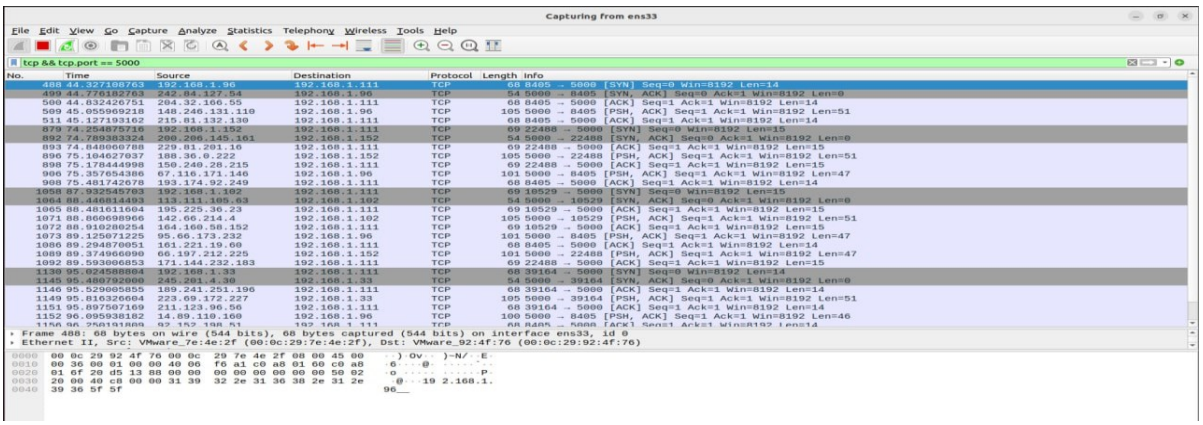

Рис. 4. Дамп Wireshark с использованием подмены адресов
Fig. 4. Wireshark dump using address substitution

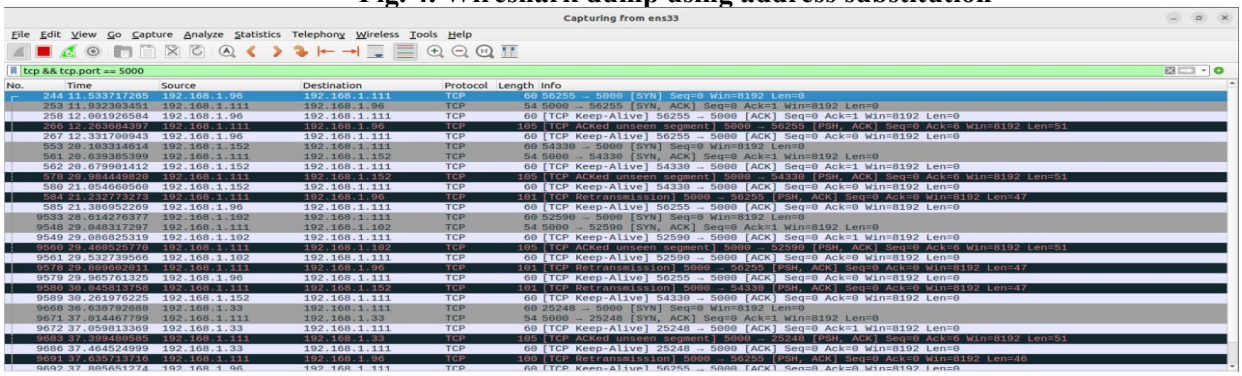

Рис. 5. Дамп Wireshark без использования подмены адресов
Fig. 5. Wireshark dump without using address substitution

При анализе дампов из приложения Wireshark можно составить конфигурацию сети, представленную на рис. 6, в способе без использования подмены адресов. Знание конфигурации сети позволяет злоумышленникам лучше планировать и осуществлять атаки, поэтому защита этой информации является критически важной для обеспечения безопасности сетевых систем [15-17].

Рис. 6. Схема корпоративной сети
Fig. 6. Corporate network diagram

Таким образом, использование данного метода способствует надежной защите корпоративных сетей от угроз, связанных с конфигурацией сети, и подтверждает необходимость внедрения инновационных подходов к обеспечению безопасности сетевых инфраструктур на основе научных принципов и технологий.

Вывод. Полученные результаты демонстрируют эффективность использования подмены адреса отправителя для повышения безопасности в корпоративных сетях. Эксперименты показали, что невозможно определить конфигурацию сети и её слабые места, что делает атаки на основе конфигурации менее вероятными. Количество пользователей постоянно растёт, и угрозы внешнего вмешательства становятся серьёзнее. Угроза несанкционированного доступа к ресурсам организации со стороны злоумышленников становится актуальной. Типичная конфигурация корпоративной сети может быть связана с соединением с Internet, что увеличивает риск внешних вторжений [18-19].

При подключении к сетям общего пользования организация сталкивается с угрозами перехвата передаваемой информации, внешних вторжений и утечек конфиденциаль-

ных данных. Безопасность корпоративных сетей можно рассматривать на нескольких уровнях информационной инфраструктуры: персонал, приложения, СУБД, ОС и сеть.

Эти результаты имеют большое значение для развития методов обеспечения безопасности в сетевых инфраструктурах. Они подтверждают необходимость применения инновационных подходов к защите корпоративных сетей от угроз, связанных с конфигурацией сети. Исследование подчёркивает значимость обеспечения безопасности в корпоративных сетях, так как они являются основой функционирования всемирной сети Internet.

Благодарности. Работа выполнена при финансовой поддержке «Грант ИБ МТУСИ» 2022 г. № 10/22-к. Соглашение № 40469-10/2022-к от 30.06.2022.

Acknowledgments. The work was carried out with the financial support of the Grant IB MTUCI 2022 No. 10/22-k. Agreement No. 40469-10/2022-k dated 06/30/2022.

Библиографический список:

1. Верещагин К.В. Защита корпоративных сетей от DDOS-атак: современные методы и тенденции // Научный лидер. 2023. - С. 12-15.
2. Пронько А.С. Анализ методов классификации трафика в сетях // Техника и технология современных производств. Пенза: Пензенский государственный аграрный университет, 2023. - С. 348-351.
3. Кистуруга А.Ю., Ковцур М.М., Шарапов Р.И. Исследование подходов к анализу чипсетов WLAN с целью выявления аппаратных уязвимостей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). - Санкт-Петербург: 2023. - С. 628-631.
4. IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE
5. Крыщенко Н.И., Миняев А.А., Ковцур М.М. Исследование рекомендаций производителей по безопасной настройке беспроводного оборудования//В сборнике: Региональная информатика и информационная безопасность. Сборник трудов Юбилейной XVIII Санкт-Петербургской международной конференции. — Санкт-Петербург, 2022. - С. 592-596.
6. Дрепа В. Е., Кистуруга А. Ю., Ковцур М.М. Точность определения местоположения WI-FI клиента в свободном пространстве при использовании индикатора уровня принимаемого сигнала//В книге: Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. - Санкт-Петербург, 2022. - С. 549-550.
7. W. Ciezobka et al., "FTMRate: Collision-Immune Distance-based Data Rate Selection for IEEE 802.11 Networks," 2023 IEEE 24th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Boston, MA, USA, 2023, pp. 242
8. Мирсаидова Н.С. Обеспечение информационной безопасности в различных сетях//Государственное управление. Национальная академия наук Таджикистана, 2023. - С. 339-347.
9. Салимгареев К.И. Защита корпоративных данных//Стратегическое развитие инновационного потенциала отраслей, комплексов и организаций. Уфа: Уфимский университет науки и технологий, 2023. С. 361-364.
10. Ченжеев Д.А. Защита информации в корпоративных компаниях//I декабрьские корпоративные чтения «Корпоративные организации: от создания до успешной деятельности». Петрозаводск: Петрозаводский государственный университет, 2022. - С. 229-233.
11. Ткачева Е.Г., Калашников В.С. Анализ атак на WI-FI сети//Научный аспект. Москва: Московский государственный технический университет имени Н.Э. Баумана, 2024. - С. 4977-4983.
12. Бейдер Дэн. Чистый Python. Тонкости программирования для профи. - Санкт-Петербург: Питер, 2020. - 288 с.
13. Васильев А.Н. Программирование на Python в примерах и задачах. - Москва: Эксмо, 2021. - 616 с.
14. Учинин А.С., Цветков А.Ю. Исследование основных характеристик и функциональных возможностей SIEM-систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). - СПБ.: 2023. - С. 910-916.
15. Игнатьева Д.А., Пестов И.Е., Федорова Е.С., Федотовская А.Д. Анализ больших данных для обеспечения информационной безопасности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). - СПБ.: 2023. - С. 567-572.
16. Петрова Т.В., Ковцур М.М., Карельский П.В., Поляничева А.В. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети//Региональная информатика (РИ-2022). - СПБ.: 2022. - С. 572-573.
17. Дрепа В.Е., Ковцур М.М., Сахаров Д.В., Шарапов Р.И. Исследование метода обнаружения атак на TDLS: анализ уязвимостей и предлагаемые решения//Региональная информатика и информационная безопасность. Сборник трудов Санкт-Петербургской международной конференции. Санкт-Петербург, 2023. - С. 375-378.
18. Крыщенко Н.И., Миняев А.А., Ковцур М.М. Исследование рекомендаций производителей по безопасной настройке беспроводного оборудования//Региональная информатика и информационная безопасность. Сборник трудов Санкт-Петербургской международной конференции. Санкт-Петербург, 2023. - С. 592-596.
19. Махмутова Н.Ф., Кистуруга А.Ю., Ковцур М.М. WIPS как основа защиты беспроводной корпоративной сети // REDS: телекоммуникационные устройства и системы. Москва: 2024.- С. 56-60.
20. Балясов А.Е., Бухарин В.В., Голуб Б.В., Кирьянов А.В., Сахаров Д.В., Стародубцев Ю.И. Способ защиты канала связи вычислительной сети. Патент на изобретение RU 2490703 C1, 20.08.2013. Заявка № 2012123121/08 от 04.06.2012.

References:

1. Vereshchagin K.V. Protection of corporate networks from DDOS attacks: modern methods and trends. *Scientific leader*. 2023; 12-15. (In Russ)
2. Pronko A.S. analysis of traffic classification methods in networks. *Technique and technology of modern productions.* - Penza: Penza state agrarian university, 2023; 348-351. (In Russ)
3. Kistruga A.Yu., Kovtsur M.M., Sharapov R.I. Research of approaches to the analysis of wlan chipsets in order to identify hardware vulnerabilities. Actual problems of infotelecommunications in science and education (APINO 2023). St. Petersburg: 2023; 628-631. (In Russ)
4. IEEE standard for information technology. Telecommunications and information exchange between systems local and metropolitan area networks. Specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (PHY) specifications," IEEE.
5. Kryshchenko N.I., Minyaev A.A., Kovtsur M.M. A study of manufacturers' recommendations for the safe configuration of wireless equipment " In the collection: regional informatics and information security. Proceedings of the XVIII Anniversary St. Petersburg international conference. St. Petersburg, 2022; 592-596. (In Russ)
6. Drepa V. E., Kistruga A. Yu., Kovtsur M.M. Accuracy of determining the location of the wi-fi client in free space when using the received signal level indicator. In the book: regional informatics (ri-2022). Jubilee XVIII st. Petersburg international conference. Conference materials. St. Petersburg, 2022; 549-550. (In Russ)
7. W. Ciezobka et al., "Ftmrate: collision-immune distance-based data rate selection for ieee 802.11 Networks," 2023 IEEE 24th international symposium on a world of wireless, mobile and multimedia networks (WoWMoM), Boston, Ma, USA, 2023; 242
8. Mirsaidova N.S. Ensuring information security in various networks. State administration. National academy of sciences of Tajikistan, 2023; 339-347.
9. Salimgareev K.I. Protection of corporate data. Strategic development of innovative potential of industries, complexes and organizations. Ufa: Ufa University of Science and Technology, 2023; 361-364. (In Russ)
10. Chenzheev D.A. Information protection in corporate companies. I december corporate readings "Corporate organizations: from creation to successful activity". Petrozavodsk: Petrozavodsk State University, 2022; 229-233. (In Russ)
11. Tkacheva E.G., Kalashnikov V.S. analysis of attacks on wi-fi networ ks. Scientific aspect. Moscow: Bauman Moscow State Technical University, 2024; 4977-4983. (In Russ)
12. Bader Dan. Pure python. The intricacies of programming for the pros. St. Petersburg: peter, 2020; 288. (In Russ)
13. Vasilyev A.N. Python programming in examples and tasks. Moscow: EKSMO, 2021; 616. (In Russ)
14. Uchinin A.S., Tsvetkov A.Yu. Research of basic characteristics and functional capabilities of SIEM systems. Actual problems of infotelecommunications in science and education (APINO 2023). St. Petersburg: 2023; 910-916. (In Russ)
15. Ignatieva D.A., Pestov I.E., Fedorova E.S., Fdotovskaya A.D. Analysis big data for information security. Actual problems of infotelecommunications in science and education . St. Petersburg: 2023; 567-572 (In Russ)
16. Petrova T.V., Kovtsur M.M., Karelsky P.V., Polyanicheva A.V. Approaches to detecting an attacker's wireless access point in a local computer network. Regional informatics (RI-2022). St. Petersburg: 2022; 572-573. (In Russ)
17. Drepa V.E., Kovtsur M.M., Sakharov D.V., Sharapov R.I. Investigation of the method of detecting attacks on tdls: vulnerability analysis and proposed solutions. Regional informatics and information security proceedings of the St. Petersburg international conference. St. Petersburg, 2023; 375-378. (In Russ)
18. Kryshchenko N.I., Minyaev A.A., Kovtsur M.M. Research of manufacturers' recommendations on safe configuration of wireless equipment. Regional informatics and information security proceedings of the St. Petersburg international conference. St. Petersburg, 2023; 592-596. (In Russ)
19. Makhmutova N.F., Kistruga A.Y., Kovtsur M.M. WIPS as the basis for protecting a wireless corporate network. *REDS: telecommunication devices and systems*. Moscow: 2024; 56-60. (In Russ)
20. Balyasov A.E., Bukharin V.V., Golub B.V., Kiryanov A.V., Sakharov D.V., Starodubtsev Yu.I. Method of protecting a communication channel of a computer network. Patent for invention RU 2490703 C1, 20.08.2013. Application No. 2012123121/08 dated 04.06.2012. (In Russ)

Сведения об авторах:

Махмутова Нурия Фаритовна, студент кафедры защищенных систем связи; iromup9898@gmail.com

Бирих Эрнест Владимирович, старший преподаватель кафедры защищенных систем связи; be1982@mail.ru. ORCID.org/0000-0003-4808-9422

Сахаров Дмитрий Владимирович, кандидат технических наук, доцент, доцент кафедры защищенных систем связи; sguard7@mail.ru. ORCID.org/0000-0002-6130-5321

Кривец Андрей Сергеевич, студент кафедры защищенных систем связи; krivets_2002@mail.ru

Дегтярев Максим Алексеевич, студент кафедры защищенных систем связи; dumbusx@gmail.com

Information about the authors:

Nuria F. Makhmutova, Student, Department of Secure Communication Systems; iromup9898@gmail.com

Ernest V. Birikh, Senior Lecturer of the Department of Secure Communication Systems; be1982@mail.ru. ORCID.org/0000-0003-4808-9422

Dmitrii V. Sakharov, Cand. Sci. (Technical), Assoc. Prof., Assoc. Prof. of the Department of Secure Communication Systems; sguard7@mail.ru. ORCID.org/0000-0002-6130-5321

Maxim A. Degtyarev, Student, Department of Secure Communication Systems; dumbusx@gmail.com

Andrey S. Krivets, Student, Department of Secure Communication Systems; krivets_2002@mail.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 20.03.2024.

Одобрена после рецензирования/ Reviced 25.04.2024.

Принята в печать/ Accepted for publication 25.04.2024.