УДК: 004.056

Романовский Степан Васильевич, студент 2 курса бакалавриата
(РГУНГ, г. Москва)

Romanovsky Stepan Vasilyevich, 2nd year student

(RSUOG, Moscow)

РЕАЛИЗАЦИЯ И АНАЛИЗ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОТ COMPROMISE INFRASTRUCTURE: NETWORK DEVICES(MITRE ATT&CK T1584.008) НА УРОВНЕ МАРШРУТИЗАТОРОВ

IMPLEMENTATION AND EFFECTIVENESS ANALYSIS OF PROTECTION AGAINST COMPROMISE INFRASTRUCTURE: NETWORK DEVICES (MITRE ATT&CK T1584.008) AT THE ROUTER LEVEL

Аннотация. В статье представлена реализация и сравнение эффективности трёх маршрутизаторов различных вендоров: Eltex, MikroTik, Cisco 1941. В ходе эксперимента была создана политика для защиты устройств от проникновения и проведено сравнение накладных расходов для прописанных правил маршрутизации.

Abstract. The article presents the implementation and comparison of the efficiency of three routers from different manufacturers: Eltex, MikroTik, Cisco 1941. During the experiment, a policy for protecting devices from intrusions was created, and a comparison was made of the overhead costs associated with implementing the specified routing rules.

ВВЕДЕНИЕ

Исследование обусловлено критической ролью в сетевой инфраструктуре для обеспечения безопасности бизнес-процессов и защиты данных предприятия. Согласно спецификации матрицы MITRE ATT&CK, техника T1584.008 описывает получение несанкционированного доступа внешней атакующей стороной, с целью долгосрочного закрепления в системе, скрытого перехвата трафика или организации повышения привилегий на горизонтальном уровне к внутренним хостам [1].

Уязвимость оборудования зачастую связана с сохранением устаревших или ненужных протоколов удаленного доступа. Перехват или извлечение конфигурационных данных позволяет атакующей стороне заменить учетные данные администраторов, что приводит к потере контроля над сегментом сети.

Ситуация осложняется при использовании корпоративных сетей в гетерогенной оболочке – то есть построенных на базе различных производителей. Каждая из систем имеет отличительные черты в механизме

защиты или передаче трафика, что усложняет аудит безопасности и требует разработки единого подхода к защите.

Объект исследования.

Интерфейсы и протоколы удаленного сетевого управления различной ИТ-инфраструктуры, построенной на базе гомогенной среды.

Предмет исследования.

Механизмы, алгоритмы и политика обеспечения информационной безопасности сетевых устройств при противодействии несанкционированному удаленному доступу (в рамках техники MITRE ATT&CK T1584.008) [1].

Цель исследования.

Повышение уровня защищенности инфраструктуры путем проведения анализа стойкости встроенных систем аутентификации оборудования и реализации политик межсетевого экрана.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Смоделировать вектор атаки на доступность подключения в изолированной среде и оценить стойкость механизмов: Cisco 1941, MikroTik CRS326-24G-2S+RM и Eltex ESR-15R.
2. Реализовать на базе маршрутизаторов политику зонирования.
3. Произвести проверку разработанных правил с использованием ОС Kali Linux.

Научная новизна работы заключается в формировании комплексного подхода к оценке защищенности инфраструктуры. В отличие исследований, сфокусированных на анализе уязвимостей конкретного вендора, в данной работе предложен сравнительный анализ систем безопасности трёх различных сетевых ОС в условиях одинаковых векторов атак.

Гипотеза исследования: предполагается, что переход от стандартных конфигураций сетевого оборудования к модели минимальных привилегий на основе разработки зонального экранирования позволит нейтрализовать риски несанкционированного удаленного управления со стороны внешнего нарушителя, независимо от стандартного уровня защиты системы хранения учетных данных конкретного производителя.

Практическая значимость исследования заключается в том, чтобы показать действенность зонального экранирования для оборудования, которые могут быть непосредственно внедрены в практику администрирования корпоративных и ведомственных сетей для минимизации угроз несанкционированного управления.

ЛИТЕРАТУРНЫЙ ОБЗОР

Официальные источники.

Согласно официальной спецификации матрицы **MITRE ATT&CK**, техника **T1584.008 (Compromise Infrastructure: Network Devices)** классифицируется как тактика *Resource Development (Разработка ресурсов)*. В данном сценарии сетевое оборудование атакуется нарушителями не ради кражи локальных данных, а для его превращения в промежуточный атакующий ресурс – для маскировки трафика (C2) [1].

Методы эксплуатации и реальные атаки.

Получение доступа администратора к прошивкам роутеров осуществляется через использование уязвимостей внешних интерфейсов, пассивного перехвата трафика или перебора пароля грубой силой. Ярким примером является активность группировки **Volt Typhoon**, которая массово компрометировала маршрутизаторы малого бизнеса для скрытой маршрутизации трафика к критической инфраструктуре. Другим примером **APT28**, где скомпрометированные сетевые устройства Ubiquiti использовались для развертывания поддельных сайтов и кражи учетных данных [2,3].

Методы защиты.

Официальные рекомендации MITRE указывают, что классические хостовые средства защиты здесь неприменимы из-за закрытости сетевых ОС. Основным методом защиты является аудит открытых портов управления и внедрение концепции зонирования **(ZBPFW)** для изоляции трафика, направленного к самому устройству. Необходимость перехода от стандартных разрешающих конфигураций к модели минимальных привилегий актуальна для всего сетевого оборудования. Как показывают недавние исследования, применение строгих политик доступа и механизмов зонального экранирования на гетерогенном оборудовании, включая Eltex ESR-15R и устройства Cisco, позволяет эффективно нейтрализовать векторы атак на плоскость управления и обеспечить требуемый уровень защищенности корпоративной инфраструктуры [4].

МАТЕРИАЛЫ И МЕТОДЫ

Теоретический анализ.

На данном этапе был проведен декомпозиционный подход к изучению архитектуры операционных систем исследуемого оборудования. Основное внимание уделялось двум факторам:

1. Архитектура разграничения доступа: Анализ алгоритмов хеширования, применяемых вендорами по умолчанию для защиты конфигурационных файлов и учетных записей администраторов.
2. Логика работы межсетевых экранов: Сопоставление классической фильтрации трафика (ACL) и объектно-ориентированного зонального экранирования (ZBPFW) с точки зрения их влияния на защищенность локальных процессов маршрутизатора.

Экспериментальное тестирование.

В эксперименте использовались три сетевых устройства и компьютеры на базе ALT/Kali Linux. Стенды подключались каждый по отдельности (2 ПК + сетевое устройство). Настраиваем порты и адреса компьютеров для последующей реализации защиты и пробы атак на устройство. Компьютер на базе ALT Linux выступает базой для управления маршрутизатором через COM-порт на маршрутизаторе.

Все параметры настройки адресации указаны в таблице для визуальной наглядности (Таблица 1).

Таблица 1. Сетевые параметры устройств на стенде

Имя устройства	Модель	Операционная система	Роль в эксперименте	IP-адрес
Eltex	Eltex ESR-15R	Eltex RouterOS v1.24.5	Настройка зон защиты (ZBPFW)	192.168.100.1 /24
Cisco	Cisco 1941	Cisco IOS v15.7(3)	Тест атаки на Telnet и хэши	10.19.103.1/24
MikroTik	CRS326-24G-2S+RM	RouterOS v7.22	Настройка зон защиты	10.19.103.1/24
Console	ПК	ALT Linux	Управление через COM-порт	10.19.103.27 port 7020
Kali-Admin	Ноутбук	Kali Linux	Легитимный администратор	10.19.103.50/24, 192.168.100.50/24
Kali-Attacker	Ноутбук	Kali Linux	Компьютер нарушителя	10.19.103.60/24, 192.168.100.2/24

В ходе практического эксперимента были развёрнуты стенды на базе оборудования трёх вендоров для проверки уязвимостей и настройки механизмов защиты. На маршрутизаторе **Cisco 1941** была смоделирована атака *перехвата трафика*: при подключении администратора по

незащищенному протоколу *Telnet,* с помощью *Wireshark* были успешно перехвачены учетные данные в виде открытого текста, после чего для защиты трафика было активировано шифрование данных и заменён telnet на протокол SSH. На **Eltex ESR-15R** была реализована защита методом зонирования трафика (***ZBPFW)***: физический интерфейс *gi1/0/2* был помещен в доверенную зону *trusted*, после чего для зон *trusted -> self* (само устройство) были созданы правила фильтрации, которые разрешили удаленный доступ по SSH исключительно с указанного IP-адреса администратора и разрешили прохождение диагностического трафика ICMP, полностью отбрасывая подключения нарушителя. На **MikroTik** защита была организована оптимизацией встроенных сетевых служб в меню *IP Services*, где были отключены неиспользуемые и небезопасные протоколы, а для оставшихся сервисов управления активированы списки контроля доступа *(allowed-from)*, ограничивающие возможность администрирования устройства только доверенной подсетью.



Рисунок 1. Блок-схема экспериментального тестирования

Анализ настройки защиты

Сравнение показало, что каждый вендор использует свои правила настройки и фильтрации устройства. Далее то, что было сделано в работе.

На **Cisco 1941** упор на замену Telnet на SSH. На **Eltex ESR-15R** реализовали зонирование *(ZBPFW)*: устройство изолируется, а доступ ограничивается по прописанным адресам. Для **MikroTik** безопасность достигается отключением лишних служб и ограничением доступа для подсетей через параметры *IP Services*. В итоге, для Cisco защищаем информацию от перехвата, в MikroTik отключаем ненужные порты/службы, Eltex обеспечивает максимальную безопасность за счет разделения сети на разные зоны.

Методология исследования

Для проверки работоспособности защиты пройдём по алгоритму из нескольких пунктов:

1. Пассивный перехват пакетов
2. Шифрование трафика/Создание правил
3. Проверка доступности и оценка защиты
4. Накладные расходы

Ограничения Исследования

Эксперимент проводится на оборудовании с версиями прошивок: **Eltex ESR-15R (Eltex RouterOS v1.24.5)**, **Cisco 1941 (Cisco IOS v15.7(3))** и **MikroTik CRS326-24G-2S+RM (RouterOS v7.22)**. Также, лабораторный стенд моделировался в изолированной среде, где всё находились в одной сети, что проще реальной инфраструктуры. Вектор атак был сужен до проверки удаленного доступа по **SSH и Telnet** (без учета Web-интерфейса, SNMP или физической консоли).

ХОД ИССЛЕДОВАНИЯ

Для каждого из стендов был применен алгоритм

1. Топология Cisco 1941

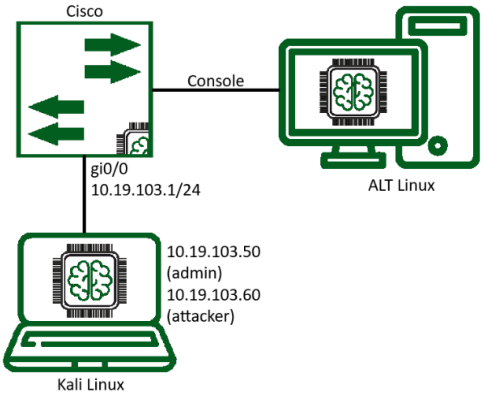


Рисунок 2. Топология Cisco 1941

1.1. **Этап атаки.** Создаём показательного пользователя (админ) через консольное подключение и указываем подключение на портах через telnet на роутере.

```
R1(config-if)#exit
R1(config)#username cisco privilege 15 password cisco123
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input telnet
R1(config-line)#exit
R1(config)#
```

Рисунок 3. Настройка пользователя + telnet-порты

1.2. Открываем на атакующем устройстве Wireshark на порту eth1 для отслеживания пакетов и авторизовываемся по telnet как администратор сети. Можем зайти на любой из пакетов и увидеть, что команды и пароли, вводимые на kali, находятся в открытом доступе. Атака проведена успешна,

атакующий может прослушивать все данные и команды, вводимые тем, кто осуществил вход в сеть.



Рисунок 4. Wireshark пакеты на Kali Linux, eth1

1.3. **Этап защиты.** Переходим обратно на консольное подключение и выстраиваем систему защиты: генерация RSA.

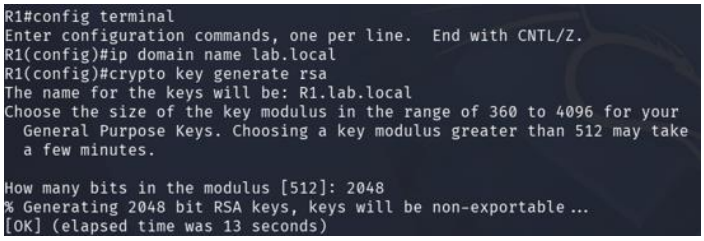


Рисунок 5. Шифрование

1.4. После генерации ключа, на портах маршрутизатора активируем протокол SSH, что блокирует возможность использования протокола Telnet.

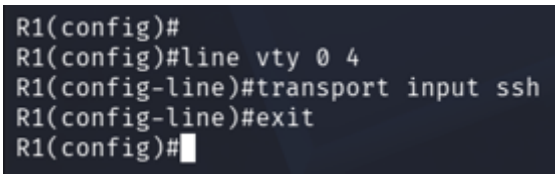


Рисунок 6. Замена telnet на ssh

1.5. Создаём список санкционированных адресов. Для эксперимента адрес 10.19.103.50 будет примером подключения администратора, остальные адреса будем отбрасывать.

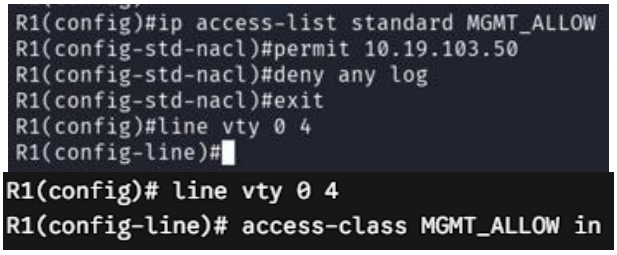


Рисунок 7. Подключили правила доступа для портов с 0 по 4

1.6. В ходе подключения с адреса отсутствующем в списке доступа, в 100% случаев при соединении маршрутизатор отказывает в подключении.

Следовательно, если адрес отсутствует в ACL, то подключение будет отбрасываться на этапе соединения, что исключает попытки перебора паролей по словарю. Аудит проверки подключений.

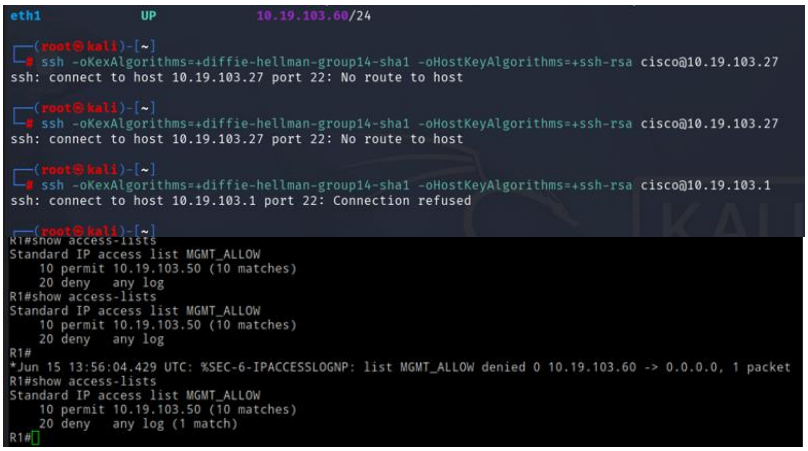


Рисунок 8-9. Аудит + попытки подключения по SSH

2. Топология MikroTik

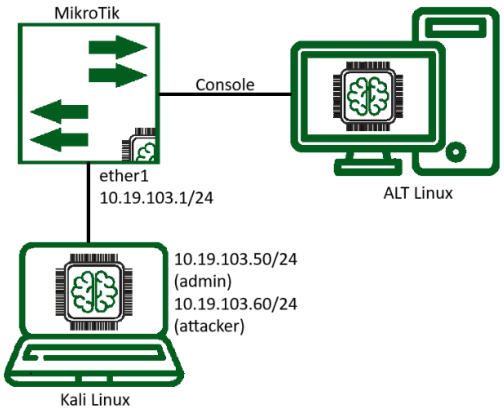


Рисунок 10. Топология MikroTik

2.1. Мы пропускаем этап пассивного перехвата трафика у MikroTik потому, что служба Telnet (TCP/23) активна в RouterOS по умолчанию, базовая конфигурация брандмауэра блокирует любые входящие запросы управления со стороны внешних интерфейсов. Кроме того, аппаратная специфика устройства (архитектура коммутации L2) изолирует широковещательный трафик сессии администрирования, делая невозможным анализ сетевых пакетов сторонним хостом без предварительного проведения атак на таблицу MAC-адресов. Пропускаем этап и настраиваем Firewall для предотвращения несанкционированного доступа. Важно записать правила фильтрации именно в порядке «сверху вниз», иначе drop заблокирует трафик раньше, чем он успеет дойти в лог.

```
[admin@MikroTik] > /ip firewall filter add chain=input src-address=10.19.103.50 action=accept comment="Allow admin Kali"
[admin@MikroTik] > /ip firewall filter add chain=input action=log log-prefix="FW-DROP" comment="Log unauthorised access"
[admin@MikroTik] > /ip firewall filter add chain=input action=drop comment="Drop everything else"
```

Рисунок 11. Настроили доступные адреса для подключения

2.2. Включаем логирование для контроля за входом в систему. Теперь можно контролировать отображение логов.

```
[admin@MikroTik] > /log print where topics~"account"
```

Рисунок 12. Вывод логов авторизации

2.3. В попытке достучаться до порта MikroTik на несанкционированном адресе, маршрутизатор не даст отправить пакеты, что делает устройство на 100% защищенным от перебора паролей грубой силой и перехвата пакетов.

```
eth1            UP              10.19.103.60/24

┌──(root㉿kali)-[~]
└─# ping -c 4 10.19.103.1
PING 10.19.103.1 (10.19.103.1) 56(84) bytes of data.

— 10.19.103.1 ping statistics —
4 packets transmitted, 0 received, 100% packet loss, time 3071ms
```

Рисунок 13. Пинги до порта микротик

```
[admin@MikroTik] > /ip firewall filter print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN  ACTION  BYTES  PACKETS
;;; Allow Admin Kali
0 input  accept  9 285      101
;;; Log unauthorized access
1 input  log     2 751       24
;;; Drop everything else
2 input  drop    2 751       24
```

Рисунок 14. С каждой попыткой несанкционированного доступа увеличение логов

3. Топология Eltex

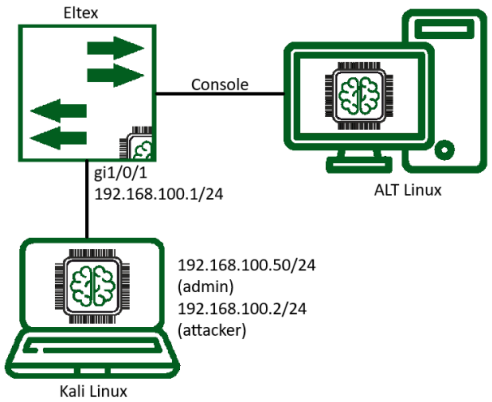


Рисунок 15. Топология Eltex

3.1. Изначально на системе Eltex порты изолированы, для соединения надо включить SSH + добавить порты в доверенную зону. Просканировать порты и перебрать пароль по словарю невозможен в силу изолированности заводских настроек.

```
esr-15r(config)# ip ssh server
```

Рисунок 16. SSH протокол включение

3.2. Устанавливаем 3 правила одно для подключения через SSH, второе разрешаем пинговать роутер санкционированному адресу (50/32) и третье отбрасываем остальные IP.

```
esr-15r(config)# security zone-pair trusted self
esr-15r(config-security-zone-pair)# rule 1
esr-15r(config-security-zone-pair-rule)# match source-address prefix 192.168.100
.50/32
esr-15r(config-security-zone-pair-rule)# action permit
esr-15r(config-security-zone-pair-rule)# enable
esr-15r(config-security-zone-pair-rule)# exit
esr-15r(config-security-zone-pair)# exit
```

Рисунок 17. Правило 1

```
esr-15r(config-security-zone-pair)# rule 2
esr-15r(config-security-zone-pair-rule)# match protocol tcp
esr-15r(config-security-zone-pair-rule)# match destination-port port-range 22
esr-15r(config-security-zone-pair-rule)# action deny
esr-15r(config-security-zone-pair-rule)# enable
esr-15r(config-security-zone-pair-rule)# exit
esr-15r(config-security-zone-pair)# exit
```

Рисунок 18. Правило 2

3.4. Проверка: подключение через SSH при отсутствующем IP в списке не дало результатов, при попытке подключения протокол зависает.

```
┌──(root㉿kali)-[~]
└─# ssh admin@192.168.100.1
^C
```

Рисунок 19. Проверка подключения

4. Накладные расходы для устройств

4.1. **Cisco 1941 (Cisco IOS) – Минимальные (~8.5% CPU).** Списки контроля доступа обрабатываются процессором программно и проверяются последовательно сверху вниз для каждого пакета. Активация ключевого слова log (команда deny any log) заставляет процессор тратить значительные ресурсы на генерацию текстовых строк для каждого отброшенного пакета нарушителя, что приводит к микрозадержкам управления.

```
CPU utilization for five seconds: 9%/8%; one minute: 5%;
```

Рисунок 20. Cisco CPU

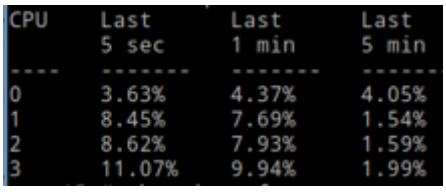
4.2. **MikroTik CRS326 (RouterOS) — Высокие (~45% CPU).** Так как это устройство серии CRS (коммутатор), трафик к самому устройству перенаправляется с аппаратного чипа на центральный процессор и обрабатывается программно. Накладные расходы вызваны правилом action=log с префиксом "FW-DROP".

```
Columns: CPU, LOAD, IRQ, DISK
#  CPU   LOAD  IRQ  DISK
0  cpu0  57%   56%  0%
1  cpu1  32%   30%  0%
```

Рисунок 21. MikroTik CPU

4.3. **Eltex ESR-15R (Eltex RouterOS) — Средние (~33% CPU).** Зонирование межсетевого экрана (ZBPFW) работает по технологии Stateful

Inspection (инспекция состояний). Процессор проверяет по правилам только *самый первый пакет* сессии, а все последующие пакеты пропускаются автоматически.



CPU	Last 5 sec	Last 1 min	Last 5 min
0	3.63%	4.37%	4.05%
1	8.45%	7.69%	1.54%
2	8.62%	7.93%	1.59%
3	11.07%	9.94%	1.99%

Рисунок 22. Eltex CPU

5. После настройки правил на сетевых оборудованиях подключение с нелигитимных адресов было невозможным.

ЗАКЛЮЧЕНИЕ

В ходе исследования было показано как уменьшить вероятность попадания злоумышленника в систему. Данная тема исследования показывает различность синтаксиса описания правил для разных вендоров. Также можно задуматься о том, что в таком случае гетерогенная система многократно увеличивает риски ошибок конфигурации и связи компонентов различных производителей.

Для проникновения в систему наиболее сложной и правильной в сборке будет гомогенный вариант сборки и выбирая из приведенного модельного ряда, предпочтительнее к установке является Eltex.

Проблематика данной уязвимости в том, что злоумышленник может поселиться в системе на долгие годы и продавать конфиденциальную информацию, либо нарушать бизнес-процессы компании, что влияет на всю систему.

Список литературы

1. Compromise Infrastructure: Network Server : technique T1584.008 // MITRE ATT&CK : [электронный ресурс]. 2026. URL: https://attack.mitre.org/techniques/T1584/008/ (дата обращения: 01.10.2026).
2. PRC State-Sponsored Cyber Actors (Volt Typhoon) Compromise SOHO Routers // Cybersecurity and Infrastructure Security Agency (CISA) : [электронный ресурс]. 2024. URL: https://www.cisa.gov/news-events/cybersecurity-advisories (дата обращения: 01.10.2026).
3. MITRE ATT&CK. Group ART28 // MITRE ATT&CK : [сайт]. — URL: https://attack.mitre.org/groups/G0007/ (дата обращения: 01.10.2026).
4. Еремина Е.А., Простова А.Н. Сравнительный анализ эффективности применения CIS Benchmark для коммутаторов Eltex в корпоративной инфраструктуре // Профессионалитет. – 2025. - №1 (005). – С. 41-59.

5. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture // NIST Special Publication 800-207. Gaithersburg : National Institute of Standards and Technology, 2020. 50 p.
6. Маршрутизаторы серии ESR. Руководство пользователя. Версия ПО 1.24 / Предприятие «ЭЛТЕКС». Новосибирск : Элтекс, 2024. 412 с. URL: https://eltex-co.ru/upload/iblock/c34/esr_user_manual_1.24.0.pdf (дата обращения: 01.10.2026).
7. Уоллам М. Руководство Cisco по безопасности сетевых устройств. М. : Вильямс, 2018. 928 с.
8. Manual: Securing your router // MikroTik Wiki : [электронный ресурс]. 2025. URL: https://help.mikrotik.com/docs/display/ROS/Securing+your+router (дата обращения: 01.10.2026).
9. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы : Учебник для вузов. 6-е изд. СПб. : Питер, 2020. 1008 с.
10. Морозова П.А. Уймин А.Г. Оценка уровня защищенности сетевых коммутаторов в современных условиях // КиберЛенинка : [электронный ресурс]. URL: https://cyberleninka.ru/article/n/otsenka-urovnya-zaschischennosti-setevyh-kommutatorov-v-sovremennyh-usloviyah (дата обращения: 01.10.2026).
11. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства : учеб. пособие / В.Ф. Шаньгин. — М. : ДМК Пресс, 2008. — 544 с. — ISBN 5-94074-383-8.
12. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учебное пособие для вузов. — М. : Академия, 2006. — 240 с. — (Высшее профессиональное образование). — ISBN 5-7695-2706-4.
13. Бородко А. В. Компьютерные сети передачи данных : учебное пособие : в 3 ч. / А. В. Бородко, Д. С. Кукунин. — Минск : БГУИР, 2019. — 3 ч.
14. Peterson L. L. Computer Networks: A Systems Approach / L. L. Peterson, B. S. Davie. — 6th ed. — Amsterdam : Morgan Kaufmann, 2021. — 832 p.
15. Крук Б. И. Телекоммуникационные системы и сети : учебное пособие для вузов : в 3 т. / Б. И. Крук, В. Н. Попантонопуло. — М. : Горячая линия – Телеком, 2012. — 3 т.