УДК 004.451.53
2.3.1. Системный анализ, управление и обработка информации



Е.А. Завадина, Т.А. Панычук
Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина

РЕАЛИЗАЦИЯ И АНАЛИЗ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОТ NETWORK SNIFFING (MITRE ATT&CK T1040) НА УРОВНЕ МАРШРУТИЗАТОРОВ

В статье представлены результаты лабораторного исследования CLI-подсценария техники Network Sniffing (MITRE ATT&CK T1040) на трех платформах маршрутизаторов: MikroTik CRS326-24G-2S+RM, Eltex ESR-15r и Cisco 810. Рассматривается сценарий скомпрометированного устройства, при котором злоумышленник использует штатные диагностические команды CLI для захвата сетевого трафика. Каждый сценарий воспроизведен 5 раз; зафиксированы время перехвата с 95-процентными доверительными интервалами, доля успешных перехватов, а также абсолютные значения утилизации CPU и RAM до и после применения защитных мер. Применен двухвыборочный t-критерий Стьюдента (поправка Уэлча) и контрольная группа с HTTPS/TLS. Все три защитные меры обеспечили нулевой процент перехвата.

Network Sniffing, MITRE ATT&CK T1040, CLI-сниффинг, MikroTik RouterOS, Eltex ESR, Cisco IOS, t-критерий Стьюдента, сетевая безопасность, импортозамещение, принцип минимальных привилегий.

Введение

Техника Network Sniffing зафиксирована в матрице MITRE ATT&CK под идентификатором T1040 в разделе тактики Credential Access (TA0006) [11]. Принципиально важно понимать, что T1040 определяется не способом получения доступа к устройству, а самим фактом перехвата сетевого трафика, проходящего через узел. MITRE ATT&CK явно разделяет эти уровни: то, как атакующий попал на устройство, описывается отдельными техниками – Initial Access или Lateral Movement. T1040 описывает именно действие – захват трафика – и прямо указывает CLI сетевого устройства как один из задокументированных векторов его реализации [11, 13]. Таким образом, SSH-доступ к маршрутизатору является предусловием атаки, а не частью самой техники T1040.

Применительно к сетевым маршрутизаторам CLI-подсценарий T1040 особенно опасен: маршрутизатор как центральный узел сети обрабатывает весь проходящий трафик, а захват пакетов через штатные команды дает атакующему доступ к данным всех устройств без дополнительного инструментария [8, 13]. В данном исследовании моделируется реалистичный сценарий скомпрометированного устройства, то есть ситуация, когда злоумышленник уже располагает SSH-доступом к маршрутизатору.

Актуальность исследования обусловлена двумя факторами. Во-первых, многие организации эксплуатируют сетевое оборудование с недостаточно проработанными политиками доступа к управляющему интерфейсу, что открывает возможность для реализации CLI-based T1040 [1, 8]. Во-вторых, в рамках политики импортозамещения российские организации переходят на отечественное оборудование класса Eltex, и вопрос сопоставимости его защитных механизмов с зарубежными аналогами остается недостаточно изученным [9].

Цель работы – экспериментально верифицировать CLI-подсценарий T1040 на трех платформах, применить к каждой специфическую защитную меру и количественно оценить ее эффективность по унифицированному набору метрик с применением методов математической статистики.

Научная новизна исследования состоит в следующем. Впервые проведен сравнительный экспериментальный анализ CLI-подсценария техники Network Sniffing одновременно на трех платформах маршрутизаторов – MikroTik CRS326-24G-2S+RM, Eltex ESR-15r и Cisco 810 – в единых контролируемых условиях с применением унифицированного набора метрик. Впервые отечественное оборудование Eltex ESR-15r включено в подобный сравнительный анализ в контексте техники T1040. Предложена и верифицирована двухуровневая защитная модель для MikroTik RouterOS, разграничивающая внешний L2-вектор и внутренний CLI-вектор (злоупотребление диагностическими командами) как два самостоятельных сценария с независимыми контрмерами. Введен единый бинарный критерий оценки результата перехвата, исключающий субъективную интерпретацию частичных результатов, и проведена статистическая обработка данных с применением двухвыборочного t-критерия Стьюдента с поправкой Уэлча и 95-процентными доверительными интервалами.

Теоретическая значимость работы заключается в уточнении интерпретации техники T1040 применительно к сетевому оборудованию: показано, что данная техника является Post-Access техникой, описы-

вающей факт перехвата трафика независимо от вектора получения доступа к устройству, а SSH-доступ к CLI маршрутизатора следует рассматривать как предусловие атаки, а не как ее составную часть. Данное разграничение устраняет методологическую неточность, встречающуюся в ряде отечественных работ по данной теме, где CLI-based сниффинг некорректно выносится за рамки T1040. Кроме того, работа расширяет теоретическую базу по применению принципа минимальных привилегий (PoLP) в контексте сетевого оборудования, демонстрируя его реализацию через платформо-специфические механизмы: политики групп пользователей RouterOS, security zone-pair в ESR OS и систему privilege levels в Cisco IOS.

Практическая значимость работы определяется тем, что результаты эксперимента могут быть непосредственно применены администраторами сетевой инфраструктуры при выборе и настройке защитных мер на оборудовании трех исследованных платформ. Для каждой платформы верифицирована конкретная конфигурация, обеспечивающая нулевой процент перехвата при накладных расходах не более 2 % CPU и 3 МБ RAM, то есть без ущерба для производительности устройства. Особую практическую ценность представляют результаты по Eltex ESR-15r: подтверждена пригодность данного оборудования для задач сетевой безопасности на уровне, сопоставимом с зарубежными аналогами, что актуально для организаций, реализующих требования по импортозамещению в соответствии с действующей нормативной базой.

В работе применялись следующие методы. Экспериментальный метод – воспроизведение атаки и защиты в контролируемой лабораторной среде с фиксированными параметрами тестового трафика и пятикратным повторением каждого сценария. Метод сравнительного анализа – сопоставление трех аппаратных платформ по единому набору метрик в идентичных условиях. Методы математической статистики – вычисление выборочного среднего, стандартного отклонения, 95-процентных доверительных интервалов на основе t-распределения Стьюдента, а также двухвыборочный t-критерий Стьюдента с поправкой Уэлча для попарного сравнения платформ. Метод контрольной группы – верификация базовой гипотезы об эффективности транспортного шифрования путем повторения эксперимента с HTTPS/TLS 1.3 и SSH-туннелем. Бинарная классификация результатов – применение единого формализованного критерия оценки («данные перехвачены» / «данные не перехвачены») для исключения субъективной интерпретации. Анализ сетевого трафика – изучение .pcap-дампов в Wireshark v.4.6.4 с применением фильтров отображения для идентификации HTTP POST-запросов и извлечения полей авторизации.

Обзор литературы

Стрельцов и Бутенко [8] систематизируют методы перехвата трафика с использованием снифферов и атак типа Man-in-the-Middle, однако работа ограничивается описательным уровнем: платформы не сравниваются, количественные метрики эффективности защиты отсутствуют. Мешкова [6] рассматривает Wireshark как аналитический инструмент без затрагивания вопросов защиты. Алексеев [1] теоретически описывает ARP-спуфинг и контрмеры на протокольном уровне без лабораторной верификации на реальном оборудовании.

Андреев [2] анализирует сетевой трафик с позиции информационной безопасности, затрагивая вопросы мониторинга, но не рассматривая сценарии атак через CLI управляемого оборудования. Демидов [4] исследует принцип минимальных привилегий применительно к серверной инфраструктуре Linux – данный подход методологически близок к защитной мере на базе групп пользователей RouterOS и разграничения привилегий Cisco IOS, примененным в настоящей работе.

Настоящее исследование дополняет перечисленные работы по нескольким направлениям. Во-первых, впервые включает отечественное оборудование Eltex ESR-15r в сравнительный анализ по технике T1040 [9]. Во-вторых, явно разграничивает вектор получения доступа и саму технику T1040, фокусируясь на CLI-подсценарии, задокументированном MITRE [11]. В-третьих, вводит единый бинарный критерий оценки результата и статистическую обработку данных. В-четвертых, включает контрольную группу с HTTPS/TLS.

Теоретические основы

Техника T1040 имеет два основных подсценария. Первый – внешний перехват – предполагает прослушивание трафика без предварительного доступа к управляемому устройству: promiscuous mode, SPAN-порт, ARP-спуфинг. Второй – внутренний (CLI-based) перехват – реализуется после получения доступа к CLI устройства через штатные диагностические команды [11, 13]. MITRE ATT&CK объединяет оба подсценария в рамках T1040, поскольку конечный результат идентичен – перехват сетевых данных – независимо от пути его достижения. В данной работе исследуется второй подсценарий.

Ключевое свойство CLI-based подсценария: маршрутизатор как центральный узел видит весь проходящий трафик, поэтому захват пакетов через его CLI дает доступ к данным всех устройств сети. SSH-доступ является предусловием атаки, а не ее составной частью – аналогично тому, как проникновение на рабочую станцию является предусловием для T1056 (Input Capture), не меняя классификацию самого действия.

Adversary-in-the-Middle (AiTM) – смежная техника внедрения в канал связи через ARP-спуфинг на уровне L2 [1]. Противодействие – статическая фиксация ARP-таблицы: переход от implicit trust к explicit trust, при которой принимаются только верифицированные записи IP→MAC. Данная мера защищает от внешнего L2-вектора атаки, но не ограничивает запуск диагностических инструментов на уровне CLI. Для защиты от CLI-подсценария T1040 на MikroTik дополнительно применяется ограничение на уровне групп пользователей RouterOS.

Принцип минимальных привилегий (PoLP) предписывает предоставлять субъекту доступ только к необходимым ресурсам [4]. В RouterOS это реализуется через политики групп пользователей: встроенная политика sniff явно контролирует доступ к /tool sniffer. В Cisco IOS – через систему уровней привилегий (privilege levels 0–15), где команды захвата трафика

выносятся на уровень 15. Оба механизма препятствуют запуску инструментов захвата трафика непривилегированными сессиями [10, 12].

Транспортное шифрование (TLS 1.3, SSH) является первичной мерой защиты от T1040 на уровне содержимого: даже при полном захвате трафика атакующий получает лишь зашифрованный поток [11]. Однако шифрование не устраняет возможность запуска диагностических инструментов на скомпрометированном маршрутизаторе, что обосновывает необходимость мер контроля доступа.

Защитные меры данного исследования воздействуют на предусловия CLI-based T1040: статическая ARP-таблица и политика sniff на MikroTik закрывают L2-вектор и CLI-вектор соответственно; IP-фильтрация SSH на Eltex блокирует несанкционированный доступ к CLI; разграничение привилегий на Cisco запрещает непривилегированным сессиям запускать команды захвата. Каждая мера блокирует цепочку атаки на этапе, предшествующем захвату трафика.

Методология эксперимента

1. Экспериментальный стенд.

Лабораторный стенд включал три физических компьютера под управлением ALT Linux Workstation 10.4 и три маршрутизатора (табл. 1). На ПК-сервере развернут Apache2 v.2.4.66 с HTML-формой авторизации, отправляющей данные методом HTTP POST. Анализ дампов выполнялся в Wireshark v.4.6.4.

Сетевая топология: два L3-сегмента – клиентская сеть 192.168.1.0/24 и серверная сеть 10.0.0.0/24. Маршрутизатор выполняет функцию шлюза. Статические маршруты: 10.0.0.0/24 via ether2, 192.168.1.0/24 via ether1. VLAN не используются. Атакующий осуществляет управление по SSH, моделируя сценарий скомпрометированного устройства.

Версии ПО маршрутизаторов: RouterOS 7.22 – актуальная стабильная версия без известных уязвимостей в механизме sniffer. ESR OS 1.24.5.5 – актуальная версия для серии ESR-15r по данным репозитория Eltex [15]. Cisco IOS 15.4(1)T достиг End of Software Maintenance в 2018 году: использование в производственной среде является самостоятельным фактором риска, независимым от T1040.

2. Объем тестового трафика.

В каждом запуске генерировалась фиксированная нагрузка: 10 HTTP POST-запросов к форме авторизации, интервал 3 секунды, длительность сессии захвата 40 секунд. Тело запроса: username=admin&password=TestPass2026 (~40 байт). Суммарный объем трафика за сессию – около 7–8 КБ с учетом TCP-заголовков и HTTP-обертки. Такой объем достаточен для надежного обнаружения POST-полей в дампе и не создает нагрузки, влияющей на ресурсные метрики.

Таблица 1

Состав экспериментального стенда и версии ПО

Роль	*Оборудование*	*IP-адрес*	*ОС / версия ПО*
Атакующий	Физический ПК	172.16.0.10	ALT Linux WS 10.4
Клиент	Физический ПК	192.168.1.10	ALT Linux WS 10.4
Сервер	Физический ПК	10.0.0.10	ALT Linux WS 10.4 + Apache2 v.2.4.66 + Python CGI
Маршрутизатор 1	MikroTik CRS326-24G-2S+RM	192.168.1.1 / 10.0.0.1	RouterOS 7.22
Маршрутизатор 2	Cisco 810	192.168.1.1 / 10.0.0.1	Cisco IOS 15.4(1)T
Маршрутизатор 3	Eltex ESR-15r	192.168.1.1 / 10.0.0.1	ESR OS 1.24.5.5

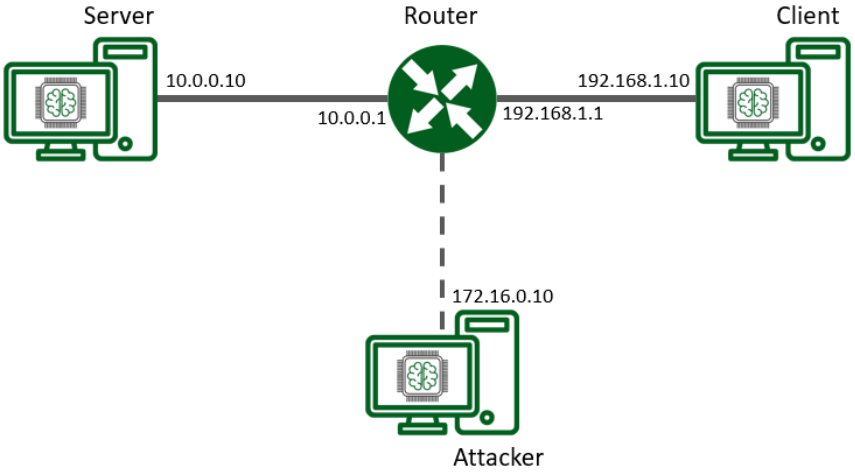


Рис. 1. Топология

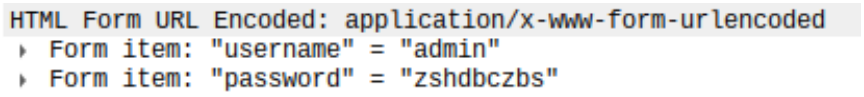


Рис. 2. Пример одного из захвата трафика

Таблица 2

Результаты контрольной группы (шифрованный трафик, n = 5)

Сценарий	*Протокол*	*Содержимое дампа*	*Итог*
Основной (атака)	HTTP	username, password открыто	Перехвачены (5/5)
Контрольный	HTTPS / TLS 1.3	TLS Handshake, зашифровано	Не перехвачены (0/5)
Контрольный	SSH-туннель	SSH-поток, зашифровано	Не перехвачены (0/5)

Таблица 3

Результаты атаки на MikroTik CRS326 (n = 5)

№	*Перехва-чены*	*Время (с)*	*CPU: база→захват*	*RAM: база→захват*	*Бинарный итог*
1	Да	3.1	4→8 %	128→134 МБ	Перехвачены
2	Да	3.4	4→7 %	128→134 МБ	Перехвачены
3	Да	2.9	4→8 %	128→135 МБ	Перехвачены
4	Да	3.5	4→9 %	128→134 МБ	Перехвачены
5	Да	3.1	4→8 %	128→134 МБ	Перехвачены
Итого	**5/5 (100 %)**	**$\bar{x}$=3.20 с; s=0.245; 95% CI [2.90; 3.50]**	**4→8±0.4 %**	**128→134±0.4 МБ**	**Данные перехвачены**

3. Критерий оценки результата.

Данные считаются «перехваченными» тогда и только тогда, когда в файле дампа присутствуют оба поля – username и password – в читаемом виде. Наличие POST-запроса без содержимого тела не является достаточным основанием для положительной классификации. По каждому из 10 запросов результат фиксируется независимо; если хотя бы в одном извлечены оба поля – запуск классифицируется как «данные перехвачены».

4. Контрольная группа.

Для верификации базовой гипотезы о роли шифрования проведена контрольная серия: веб-сервер переведен в режим HTTPS (TLS 1.3), протестирован сценарий с SSH-туннелем. Дамп захватывался тем же инструментом на MikroTik. Результаты – в таблице 2.

При использовании HTTPS и SSH в дампе фиксировались только метаданные соединения, но не содержимое. Это подтверждает эффективность транспортного шифрования как первичной меры защиты от T1040 [11]. Вместе с тем при наличии CLI-доступа атакующий сохраняет возможность видеть метаданные трафика, что обосновывает необходимость мер контроля доступа.

5. Статистическая обработка.

По каждой платформе вычислялись: выборочное среднее ($\bar{x}$), стандартное отклонение (s), стандартная ошибка (SE = s/√n) и 95-процентный доверительный интервал по формуле $\bar{x} \pm t_{0.05} \times SE$, где $t_{0.05} = 2.776$ при df = 4. Для попарного сравнения применен двухвыборочный t-критерий Стьюдента с поправкой Уэлча. Критическое значение |t| при α = 0.05 и df ≈ 5–7 составляет ~2.57.

Результаты экспериментов

1. MikroTik CRS326-24G-2S+RM.

Атака. С ПК-атакующий по SSH активирован встроенный sniffer RouterOS (/tool sniffer): фильтр TCP/HTTP, все интерфейсы, файл capture.pcap. После отправки тестовых запросов файл передан по TFTP. В Wireshark во всех 5 запусках обнаружены поля username и password в открытом виде. Базовая утилизация ресурсов MikroTik CRS326 в состоянии покоя: CPU 4 %, RAM 128 МБ.

Защита. Применены две независимые меры для двух векторов атаки.

Мера 1 (внешний L2-вектор): статическая фиксация ARP-таблицы – для каждого доверенного устройства внесена запись IP→MAC с атрибутом permanent, динамическое обновление ARP отключено. Данная мера предотвращает перехват трафика путем ARP-спуфинга, однако не ограничивает доступ к CLI и не препятствует запуску /tool sniffer при наличии SSH-доступа.

Мера 2 (CLI-вектор): ограничение политики sniff через группы пользователей RouterOS. Создана пользовательская группа с явным исключением политики sniff из набора разрешений. При попытке запуска /tool sniffer из сессии с ограниченными правами RouterOS возвращает ошибку доступа. Данная мера непосредственно блокирует CLI-подсценарий T1040.

После применения обеих мер эксперимент был повторен 5 раз. Результаты представлены в таблице 4.

Накладные расходы на поддержание статической ARP-таблицы и пользовательских групп: CPU +1 %, RAM +2 МБ относительно базовых значений.

2. Eltex ESR-15r.

Атака. Активирован инструмент monitor на интерфейсе gi1/0/1 (ESR OS 1.24.5.5). Файл передан по FTP. В Wireshark обнаружены HTTP POST с полями авторизации. Базовая утилизация Eltex ESR-15r в состоянии покоя: CPU 8 %, RAM 256 МБ. Наибольшее стандартное отклонение среди трех платформ (s = 0.447 с) объясняется вариабельностью планировщика процессов ESR OS при параллельной маршрутизации.

Защита. В конфигурации security zone-pair задано правило: SSH (TCP/22) разрешен только с адреса 172.16.0.1; все остальные подключения блокируются правилом Deny. TCP SYN с адреса атакующего отклоняется до этапа аутентификации. Запуск monitor во всех 5 попытках недоступен. Накладные расходы: CPU +2 %, RAM +3 МБ.

3. Cisco 810.

Атака. Использована команда monitor capture (Cisco IOS EPC, версия 15.4(1)T). Дамп передан по FTP. Базовая утилизация Cisco 810 в состоянии покоя: CPU 6 %, RAM 256 МБ. Во всех 5 запусках обнаружены поля username и password. Наибольшие время перехвата ($\bar{x}$ = 5.24 с) и дисперсия (s = 0.702 с) обусловлены программной реализацией EPC на MIPS-процессоре при высокой утилизации CPU (14 %).

Таблица 4

Результаты защиты на MikroTik CRS326 (n = 5, две меры)

№	*Перехвачены*	*Время реакции (с)*	*sniff заблокирован*	*Итог*
1	Нет	< 1	Да	Не перехвачены
2	Нет	< 1	Да	Не перехвачены
3	Нет	< 1	Да	Не перехвачены
4	Нет	< 1	Да	Не перехвачены
5	Нет	< 1	Да	Не перехвачены
Итого	**0/5 (0 %)**	**< 1 с**	**5/5 (100 %)**	**Данные не перехвачены**

Таблица 5

Результаты атаки на Eltex ESR-15r (n = 5)

№	*Перехвачены*	*Время (с)*	*CPU: база→захват*	*RAM: база→захват*	*Бинарный итог*
1	Да	4	8→11 %	256→264 МБ	Перехвачены
2	Да	4.8	9→12 %	256→264 МБ	Перехвачены
3	Да	3.9	8→11 %	256→265 МБ	Перехвачены
4	Да	4.2	8→10 %	256→264 МБ	Перехвачены
5	Да	3.6	9→11 %	256→264 МБ	Перехвачены
Итого	**5/5 (100 %)**	**$\bar{X}$=4.10 с; s=0.447; 95 % CI [3.54; 4.66]**	**8→11±0.7 %**	**256→264±0.4 МБ**	**Данные перехвачены**

Таблица 6

Результаты атаки на Cisco 810 (n = 5)

№	*Перехвачены*	*Время (с)*	*CPU: база→захват*	*RAM: база→захват*	*Бинарный итог*
1	Да	5.1	6→14 %	256→266 МБ	Перехвачены
2	Да	6.4	6→15 %	256→267 МБ	Перехвачены
3	Да	5	6→13 %	256→266 МБ	Перехвачены
4	Да	5.2	6→14 %	256→266 МБ	Перехвачены
5	Да	4.5	6→14 %	256→266 МБ	Перехвачены
Итого	**5/5 (100 %)**	**$\bar{x}$=5.24 с; s=0.702; 95 % CI [4.37; 6.11]**	**6→14±0.7 %**	**256→266±0.4 МБ**	**Данные перехвачены**

Таблица 7

Результаты попарного t-теста (критерий Уэлча, α = 0.05)

Пара платформ	*|t| (Уэлч)*	*df*	*p < 0.05?*	*Вывод*
MikroTik vs Eltex	3.947	6.2	Да	Различие статистически значимо
MikroTik vs Cisco	6.134	5.0	Да	Различие статистически значимо
Eltex vs Cisco	3.062	6.8	Да	Различие статистически значимо

Таблица 8

Итоговое сравнение трех платформ (n = 5 на каждую)

Маршрутизатор	*Без защиты*	*Время перехвата, 95 % CI*	*С защитой*	*t реакции*	*CPU / RAM (защита)*
MikroTik CRS326	5/5	3.20 с [2.90; 3.50]	0/5	< 1 с	+1 % CPU / +2 МБ
Eltex ESR-15r	5/5	4.10 с [3.54; 4.66]	0/5	< 1 с	+2 % CPU / +3 МБ
Cisco 810	5/5	5.24 с [4.37; 6.11]	0/5	< 1 с	+1 % CPU / +1 МБ

Защита. Команда monitor capture вынесена на уровень привилегий 15 (enable), недоступный пользовательским сессиям [10]. При попытке выполнения IOS возвращает «% Invalid input detected at '^' marker». Все 5 попыток зафиксированы в системном журнале. Накладные расходы: CPU +1%, RAM +1 МБ.

Статистический анализ

95-процентные доверительные интервалы для среднего времени перехвата: MikroTik – [2.90; 3.50] с, Eltex – [3.54; 4.66] с, Cisco – [4.37; 6.11] с. Интервалы не перекрываются, что предварительно указывает на значимые различия между платформами. Результаты попарного t-теста приведены в таблице 7.

Во всех трех парах |t| превышает критическое значение (~2.57), что подтверждает статистическую значимость различий. MikroTik быстрее Eltex на 0.90 с (|t| = 3.947), Eltex быстрее Cisco на 1.14 с (|t| = 3.062), MikroTik быстрее Cisco на 2.04 с (|t| = 6.134). Различия отражают архитектурные особенности платформ: аппаратное ускорение sniffer в RouterOS против программной реализации EPC на MIPS-процессоре у Cisco. Следует учитывать, что при n = 5 статистическая мощность критерия ограничена; результаты носят предварительный характер.

Дисперсия метрик ресурсопотребления: CPU – MikroTik σ = 0.45 %, Eltex σ = 0.71 %, Cisco σ = 0.71 %; RAM – все платформы σ = 0.45 МБ. Низкие значения подтверждают стабильность условий эксперимента.

Обсуждение результатов

Сводные данные по всем платформам с 95-процентными доверительными интервалами приведены в таблице 8.

Все три маршрутизатора подтвердили реализуемость CLI-подсценария T1040: штатные диагностические инструменты позволяют перехватывать учетные данные в течение 3–6 секунд после начала сессии. Это согласуется с описанием техники в MITRE ATT&CK [11] и подтверждает практическую применимость CLI-based вектора как инструмента разведки при наличии доступа к маршрутизатору.

Для MikroTik применена комплексная двухуровневая защита. Статическая ARP-таблица эффективно закрывает внешний L2-вектор, однако не препятствует захвату трафика при наличии CLI-доступа – это является принципиальным ограничением данной меры в контексте CLI-подсценария T1040. Ограничение политики sniff через группы пользователей RouterOS непосредственно блокирует CLI-вектор: попытка запуска /tool sniffer завершается ошибкой доступа вне зависимости от иных настроек. Совместное применение обеих мер обеспечивает полное покрытие обоих векторов атаки.

На Eltex и Cisco применены меры, воздействующие непосредственно на предусловия CLI-доступа и на привилегии внутри сессии соответственно. Все три подхода показали одинаковую эффективность – 0/5 перехватов – при различных накладных расходах: Eltex несет наибольшие расходы (+2 % CPU, +3 МБ), MikroTik и Cisco – минимальные (+1 % CPU, +1–2 МБ).

Результаты Eltex ESR-15r подтверждают пригодность отечественного оборудования для задач сетевой безопасности в рамках политики импортозамещения [9]: механизм security zone-pair обеспечил полную блокировку атаки с накладными расходами, сопоставимыми с зарубежными аналогами.

Ограничения работы: изолированная лабораторная среда с минимальной фоновой нагрузкой; n = 5 ограничивает статистическую мощность; примененные меры не исчерпывают возможные контрмеры (не рассматриваются детализированный аудит команд CLI, RADIUS-аутентификация, мониторинг аномалий).

Заключение

В работе экспериментально подтверждена реализуемость CLI-подсценария техники T1040 (MITRE ATT&CK) на трех классах маршрутизаторов. Установлено, что T1040 определяется фактом перехвата трафика, а не способом получения доступа к устройству: SSH-доступ является предусловием атаки в рамках CLI-подсценария, задокументированного MITRE [11].

Статистический анализ выявил значимые различия во времени перехвата: MikroTik – 3.20 с [2.90; 3.50], Eltex – 4.10 с [3.54; 4.66], Cisco – 5.24 с [4.37; 6.11]. Для каждой платформы верифицирована защитная мера, обеспечившая 100-процентную блокировку перехвата во всех 15 экспериментах. Для MikroTik применена двухуровневая защита: статиче-

ская ARP-таблица закрывает внешний L2-вектор, ограничение политики sniff через группы пользователей – CLI-вектор. Для Eltex – IP-фильтрация SSH через security zone. Для Cisco – разграничение привилегий на уровне IOS. Накладные расходы не превысили 2 % CPU и 3 МБ RAM.

Отечественное оборудование Eltex ESR-15r показало результаты, полностью сопоставимые с зарубежными аналогами по эффективности защиты, что подтверждает его применимость при реализации требований по импортозамещению [9]. Контрольная группа с HTTPS/TLS подтвердила базовую гипотезу об эффективности транспортного шифрования как первичной меры защиты от T1040. Направлением дальнейших исследований является тестирование под производственной нагрузкой, увеличение объема выборки до $n \geq 30$ и анализ устойчивости к зашифрованным C2-каналам.

Литература

1. Алексеев, А. П. Защита от атак типа человек посередине / А. П. Алексеев. – Текст : электронный // Вестник МГТУ МИРЭА. – 2015. – URL: https://cyberleninka.ru/article/n/zaschita-ot-atak-tipa-chelovek-poseredine (дата обращения: 03.04.2026).

2. Андреев, Р. И. Анализ сетевого трафика с целью обеспечения информационной безопасности / Р. И. Андреев. – Текст : электронный // Молодой ученый. – 2020. – URL: https://cyberleninka.ru/article/n/analiz-setevogo-trafika-s-tselyu-obespecheniya-informatsionnoy-bezopasnosti (дата обращения: 03.04.2026).

3. Беляев, П. А. Системы мониторинга и анализа сетевого трафика / П. А. Беляев // Форум молодых учёных. – 2021. – № 4. – С. 112–119.

4. Демидов, Р. А. Методы повышения безопасности при администрировании серверов Linux / Р. А. Демидов // Вопросы кибербезопасности. – 2025. – URL: https://cyberleninka.ru/article/n/metody-povysheniya-bezopasnosti-pri-administrirovanii-serverov-linux (дата обращения: 03.04.2026).

5. Закомолдин, С. Д. Анализ сетевых протоколов для выявления угроз: современные методы и проблемы / С. Д. Закомолдин // Вестник науки. – 2025. – № 4. – С. 45–58.

6. Мешкова, Е. В. Перехват и анализ сетевого трафика с помощью Wireshark / Е. В. Мешкова // Молодой ученый. – 2016. – URL: https://cyberleninka.ru/article/n/perehvat-i-analiz-setevogo-trafika-s-pomoschyu-wireshark (дата обращения: 02.04.2026).

7. Михайлов, А. Н. Обнаружение аномалий в сетевом трафике с использованием методов машинного обучения / А. Н. Михайлов // Вестник науки. – 2024. – № 4. – С. 78–89.

8. Стрельцов, Д. С. Анализ и методика проведения перехвата сетевого трафика. Методы защиты / Д. С. Стрельцов, Е. А. Бутенко // Вопросы кибербезопасности. – 2024. – URL: https://cyberleninka.ru/article/n/analiz-i-metodika-provedeniya-perehvata-setevogo-trafika (дата обращения: 03.04.2026).

9. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 «Сетевое и системное администрирование». Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. – 2025. – № 11(628). – С. 58–62. – EDN DMHQJU.

10. Cisco Systems. Embedded Packet Capture Configuration Guide. – URL: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-embedded-packet-capture/116045-productconfig-epc-00.html (дата обращения: 03.04.2026). – Text : electronic.

11. MITRE ATT&CK. Technique T1040: Network Sniffing. – URL: https://attack.mitre.org/techniques/T1040/ (дата обращения: 01.04.2026). – Text : electronic.

12. MikroTik. Packet Sniffer – RouterOS Documentation. – URL: https://help.mikrotik.com/docs/display/ROS/Packet+Sniffer (дата обращения: 03.04.2026). – Text : electronic.

13. PT Security. MITRE ATT&CK: Техника T1040 – Прослушивание сетевого трафика. – URL: https://service.securitm.ru/mitre/techniques/T1040 (дата обращения: 04.04.2026). – Текст : электронный.

14. ООО «Элтекс». Настройка zone-based firewall на маршрутизаторах ESR. – 2025. – URL: https://eltexcm.ru/baza-znanij/esr/primer-nastrojki/bezopasnostfiltraciya/esr-konfigurirovanie-firewall.html (дата обращения: 04.04.2026). – Текст : электронный.

15. ООО «Элтекс». Руководство по эксплуатации маршрутизаторов серии ESR. Версия 4.0. – Новосибирск : Элтекс, 2025. – URL: https://docs.eltex-co.ru/esr/operation_manual (дата обращения: 03.04.2026). – Текст : электронный.

E.A. Zavadina, T.A. Panychuk

Gubkin Russian State University of Oil and Gas

(National Research University)

IMPLEMENTATING AND ANALYSING THE EFFECTIVENESS OF PROTECTION AGAINST NETWORK SNIFFING (MITRE ATT&CK T1040) AT THE ROUTER LEVEL

This article presents the results of a laboratory study regarding the CLI sub-scenario of the Network Sniffing technique (MITRE ATT&CK T1040) across three router platforms: MikroTik CRS326-24G-2S+RM, Eltex ESR-15r, and Cisco 810. The study examines a compromised device scenario in which an attacker utilizes standard CLI diagnostic commands to capture network traffic. Each scenario was replicated five times; recorded metrics included capture duration (with 95% confidence intervals), the success rate of captures, and absolute CPU and RAM utilization values before and after the implementation of protective measures. A two-sample Student's t-test (Welch's correction) was applied, utilizing an HTTPS/TLS-based control group. All three protective measures resulted in a zero percent capture rate.

Network Sniffing, MITRE ATT&CK T1040, CLI sniffing, MikroTik RouterOS, Eltex ESR, Cisco IOS, Student's t-test, network security, import substitution, principle of least privilege.