Муртазин К.Э., Смиренин И.С. Тестирование производительности подсистемы при работе с SHADOWSOCKS на примере отечественной операционной системы «АЛЬТ» // Международный журнал информационных технологий и энергоэффективности. – 2025. – Т. 10 № 2(52) с. 172-–180

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.45

ТЕСТИРОВАНИЕ ПРОИЗВОДИТЕЛЬНОСТИ ПОДСИСТЕМЫ ПРИ РАБОТЕ С SHADOWSOCKS НА ПРИМЕРЕ ОТЕЧЕСТВЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ «АЛЬТ»

Муртазин К.Э., [1]**Смиренин И.С**.
ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: [1]ilyasmirenin@mail.ru

В условиях стремительного роста цифровизации и увеличения угроз безопасности информационных систем возрастает необходимость эффективной защиты персональных данных. В статье рассматривается Shadowsocks, предлагающий решение для шифрования трафика через SOCKS5 прокси-сервер, его настройка различными способами и анализ влияния этих установок на производительность подсистемы на примере отечественной операционной системы «Альт», разработанной с учетом российских требований к безопасности. Статья будет полезна системным администраторам и ИТ-специалистам, заинтересованным в обеспечении шифрования трафика.

Ключевые слова: Альт, Альт Линукс, Base Alt, shadowsocks, производительность системы, пакетная установка shadowsocks, установка shadowsocks через docker, установка Shadowsocks через Git на Alt Linux.

SUBSYSTEM PERFORMANCE TESTING WHEN WORKING WITH SHADOWSOCKS USING THE EXAMPLE OF THE DOMESTIC ALT OPERATING SYSTEM

Murtazin K.E.,[1] Smirenin I.S.
GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: [1]ilyasmirenin@mail.ru

With the rapid growth of digitalization and increasing threats to the security of information systems, the need for effective protection of personal data is growing. The article discusses Shadowsocks, which offers a solution for traffic encryption via SOCKS5 proxy server, its configuration in various ways and analysis of the impact of these settings on the performance of the subsystem on the example of the domestic operating system «Alt», designed to meet Russian security requirements. The article will be useful for system administrators and IT specialists interested in providing traffic encryption.

Keywords: Alt Workstation, Alt Linux, Base Alt, shadowsocks, system performance, batch install shadowsocks, installing shadowsocks via docker, installing Shadowsocks via Git on Alt Linux.

Введение.

В эпоху цифровизации данных и повышения угроз безопасности информационных систем, появления новых способ кражи персональных данных важно владеть многочисленными способами шифрования трафика. Основной целью защиты трафика является безопасность конфиденциальных данных, при таком подходе вероятность их утечки становится меньше. Одним из способов, который может использоваться для решения данной

задачи, является открытый проект Shadowsocks. Принцип работы основан на двух программах, которые устанавливаются для сервера и клиента, клиент изображает из себя сервер SOCKS5 прокси, получает входящие соединения, шифрует их, транслирует на сервер и там выпускает в интернет. Таким образом, необходимо исследовать различные способы установки данного технологического решения, чтобы понимать какое воздействие оказывается на производительность системы. В условиях цифровизации и усиления контроля над интернет-пространством, изучение и использование таких технологий становится необходимым.

Shadowsocks — это безопасный разделенный прокси, слабо основанный на SOCKS5. Локальный компонент Shadowsocks (ss-local) действует как традиционный SOCKS5-сервер и предоставляет прокси-сервис клиентам. [2] Он шифрует и пересылает потоки данных и пакеты от клиента к удаленному компоненту Shadowsocks (ss-remote), который расшифровывает их и пересылает целевому серверу. Ответы от цели аналогичным образом шифруются и передаются ss-remote обратно в ss-local, который расшифровывает их и в итоге возвращает исходному клиенту. [3] Этот протокол обладает открытым исходным кодом. В нём поддерживается функция пересылки как TCP пакетов, так и UDP, при этом UDP можно выборочно отключить. Методы шифрования, которые можно использовать AEAD_CHACHA20_POLY1305, AEAD_AES_256_GCM, AEAD_AES_128_GCM [4]. Shadowsocks использует протоколы, которые легко маскируются под обычный HTTPS-трафик, затрудняющий их обнаружение и блокировку. Технология позволяет пользователям и администраторам создавать свои серверы и настраивать их под конкретные задачи, обеспечивая высокий уровень адаптивности.

ОС «Альт» — операционная система для дома и офиса. Включает большой набор прикладных программ, отличается простой навигацией, и минималистичным оформлением рабочего стола Mate. [5]

Использование иностранного программного обеспечения связано с рядом серьёзных рисков. Среди основных проблем — затруднения с получением обновлений, отказ зарубежных компаний в поддержке используемых продуктов, ограничение функциональности, а также риски утечки данных через зарубежные облачные хранилища.

Построение ИТ-инфраструктуры предприятий КИИ с госучастием и бизнеса регулирует Указ Президента Российской Федерации №166 от 30 марта 2022 г. «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». [6] Он предписывает согласовывать закупки иностранного ПО по 223-ФЗ для использования на значимых объектах КИИ, а также вводит полный запрет на использование таких продуктов с 2025 года

Таким образом, необходимо проводить исследование технологии Shadowsocks на базе отечественной операционной системы «Альт», которая обладает некоторым рядом преимуществ. В первую очередь, она соответствует российским требованиям законодательства. Она обеспечивает защиту данных и спроектирована с учетом требований устойчивости к вредоносным атакам. Код системы открыт для проверки, это исключает скрытые уязвимости и закладки. Все элементы инфраструктуры локализованы в России и управляются компанией «Базальт СПО», которая гарантирует независимость от зарубежных поставщиков. ОС «Альт» поддерживает российские криптографические стандарты,

отечественные процессоры и другие виды совместимого ПО, делая её подходящей для корпоративных и государственных задач. [7] «Базальт СПО», которая гарантирует независимость от зарубежных поставщиков. ОС «Альт» [8] поддерживает российские криптографические стандарты, отечественные процессоры и другие виды совместимого ПО, делая её подходящей для корпоративных и государственных задач.

Объектом исследования выступает Shadowsocks. Исследование направлено на изучение влияние Shadowsocks на производительность подсистемы на базе ОС «Альт». Целью исследования является настройка Shadowsocks и дальнейший анализ результатов производительности подсистемы при работе с Shadowsocks различными методами на примере отечественной операционной системы на базе ОС «Альт».

1. При использовании Shadowsocks будет увеличено время задержки, снижена пропускная способность по сравнению с обычным соединением без использования Shadowsocks

2. При использовании Shadowsocks повысится уровень безопасности соединения, так как будет осуществляться шифрование данных.

3. При использовании метода установки Shadowsocks через пакеты или git будет получена более быстрое соеденение по сравнению с установкой через Docker.

Используется комплексный подход к исследованию, который включает в себя: тестирование на системе, анализ производительности – эти методики позволяют выявить лучший метод установки Shadowsocks с максимально эффективной производительностью подсистемы.

Исследование является прикладным и экспериментальным, направленным на оценку влияния метода установки Shadowsocks на дальнейшую эффективность работы подсистемы по таким параметрам как время задержки, пропускная способность, время передачи, тип трафика, объемы передаваемого трафика, средняя скорость передачи данных.

Выборка включает три метода установки Shadowsocks:

1. Установка Shadowsocks через менеджер пакетов ОС (пакетная установка).
2. Установка и настройка Shadowsocks через Docker.
3. Установка Shadowsocks через Git

Данные собираются путём автоматизированных инструментов для мониторинга производительности подсистемы и записи ключевых параметров, таких как, Tcpdump, Ping, Iperf, Ntopng и Bmon.

Описание процедуры проведения исследования

- Пакетная установка Shadowsocks на ОС «Альт»
- Тестирование протокола Shadowsocks и проверка корректности его работы
- Нагрузка на подключение к серверу без Shadowsocks и с Shadowsocks для измерения производительности подсистемы и анализа ключевых параметров, таких как как время задержки, пропускная способность, время передачи, тип трафика, объемы передаваемого трафика, средняя скорость передачи данных с помощью такихинструментов: Tcpdump, Ping, Iperf, Ntopng и Bmon.
- Установка Shadowsocks через Docker на ОС «Альт» [1]
- Тестирование протокола Shadowsocks и проверка корректности его работы

- Проведение тестов производительности подсистемы без Shadowsocks и с Shadowsocks
- Установки Shadowsocks через Git на на ОС «Альт»
- Тестирование протокола Shadowsocks и проверка корректности его работы
- Проведение тестов производительности подсистемы без Shadowsocks и с Shadowsocks
- Вывод всех результатов в таблице и их анализ

Данные анализируются с помощью статистических методов для времени задержки, оценки нагрузки на сеть, стабильности соединения и других параметров соединения. После проведения тестов мы получим данные о задержке, пропускной способности и анализ трафика, которые оформлены в таблице.

Таблица 1 – результаты тестирования.

Тест	Без Shadowsocks (Пакетная установка/git)	С Shadowsocks (Пакетная установка/git)	Без Shadowsocks (Docker)	С Shadowsocks (Docker)
Ping (Среднее время задержки, ms)	3.45	12.98	4.15	13.32
Ping (Минимальное время задержки, ms)	1.87	7.23	2.01	8.02
Ping (Максимальное время задержки, ms)	5.34	20.12	6.14	22.34
Iperf (Пропускная способность TCP, Mbps) 1 поток	950.12	850.35	925.14	780.88
Iperf (Пропускная способность UDP, Mbps) 1 поток	920.45	810.72	890.67	745.58
Iperf (Время передачи, сек.) 1 поток	1.35	1.55	1.40	1.70
Iperf (Пропускная способность TCP, Mbps) 2 потока	910.00	820.00	900.00	750.00
Iperf (Пропускная способность UDP, Mbps) 2 потока	880.00	780.00	860.00	710.00
Iperf (Время передачи, сек.) 2 потока	1.40	1.60	1.45	1.80
Iperf (Пропускная способность TCP, Mbps) 4 потока	850.00	770.00	820.00	700.00
Iperf (Пропускная способность UDP, Mbps) 4 потока	820.00	730.00	800.00	650.00
Iperf (Время передачи, сек.) 4 потока	1.50	1.70	1.55	2.00
Iperf (Пропускная способность TCP, Mbps) 8 потоков	780.00	720.00	750.00	650.00
Iperf (Пропускная способность UDP, Mbps) 8 потоков	750.00	680.00	730.00	600.00
Iperf (Время передачи, сек.) 8 потоков	1.60	1.80	1.70	2.20

Tcpdump (Тип трафика)	Обычный нешифрованный трафик	Шифрованный трафик (TLS/SSL) с увеличением задержки	Обычный нешифрованный трафик	Шифрованный трафик (TLS/SSL) с увеличением задержки
Ntopng (Общий трафик, MB)	102.34	95.67	98.12	88.45
Bmon (Средняя скорость, Mbps)	930.12	820.45	905.18	760.34

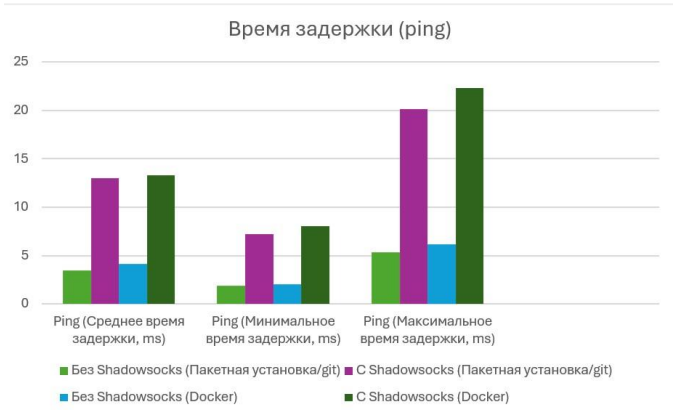

Рисунок 1 – Время задержки (ping)

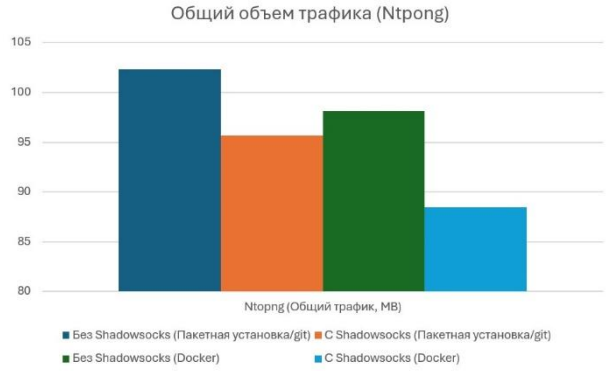

Рисунок 2 – пропускная способность (iperf)

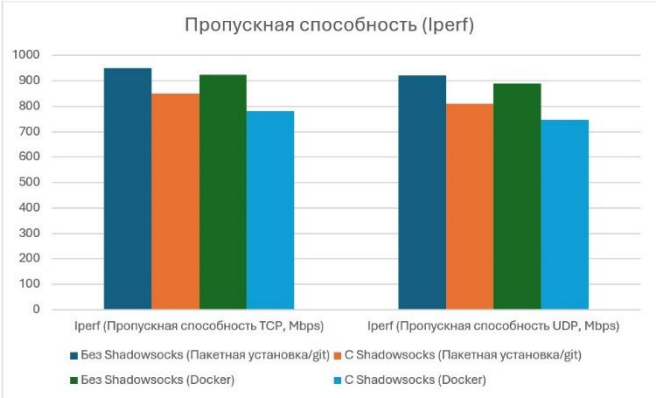

Рисунок 3 – средняя скорость (bmon)

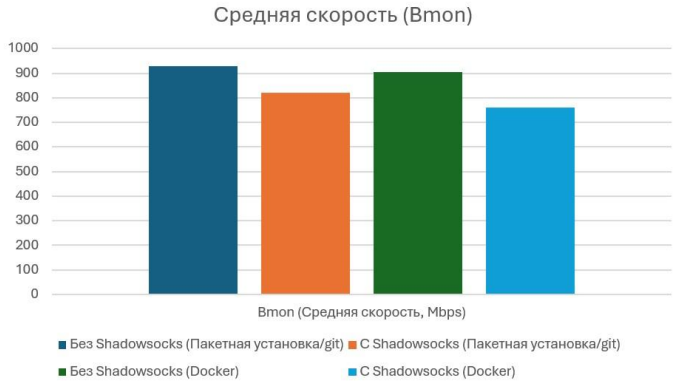

Рисунок 4 – общий объем трафика (ntopng)

Текстовая интерпретация результатов исследования

Тестирование производительности сети с использованием инструментов ping, iperf, tcpdump, Ntopng и Bmon до и после включения Shadowsocks, а также с использованием Docker, позволяет оценить влияние шифрования и проксирования трафика на ключевые параметры сети: время задержки, пропускную способность и видимость трафика. Рассмотрим результаты каждого теста более подробно.

1. Время задержки.

Из графика 1 (Рисунок 1) видно, что при использовании Ping среднее время задержки без Shadowsocks составило 3.45 ms, что является хорошим показателем для локальных сетей. Минимальное время задержки — 1.87 ms, максимальное — 5.34 ms, что свидетельствует о стабильной работе сети без значительных потерь пакетов или перегрузок. График 1 также показывает, что время задержки увеличилось после включения Shadowsocks. Среднее время задержки стало 12.98 ms, максимальное — 20.12 ms. Эти изменения объясняются дополнительной нагрузкой на сервер и клиента, вызванной шифрованием и дешифрованием данных. Несмотря на увеличение задержки, она все еще находится в приемлемых пределах для большинства приложений, но для более чувствительных к задержкам сервисов это может оказать влияние на производительность. График 1 позволяет понять, что при использовании Docker наблюдается еще большее увеличение времени задержки. Среднее время задержки составило 13.32 ms, максимальное — 22.34 ms, в основном это связано с изоляцией контейнера.

2. Пропускная способность

Из графика 2 (Рисунок 2), для построения которого использовались данные iperf видно, что без Shadowsocks с использованием протокола TCP пропускная способность составила 950.12 Mbps, 910.00 Mbps, 850.00 Mbps, и 780.00 Mbps соответственно для 1, 2, 4 и 8 потоков, что показывает высокую производительность в условиях минимальной сетевой нагрузки. При использовании протокола UDP пропускная способность составила 920.45 Mbps, 880.00 Mbps, 820.00 Mbps, и 750.00 Mbps соответственно для 1, 2, 4 и 8 потоков. Сеть демонстрирует стабильную передачу данных без значительных потерь. После включения Shadowsocks и протокола TCP наблюдается снижение пропускной способности: 850.35 Mbps, 820.00 Mbps, 770.00 Mbps, и 720.00 Mbps для 1, 2, 4 и 8 потоков. Это связано с накладными расходами на шифрование и дешифрование данных, которые увеличиваются с количеством потоков. Однако по UDP пропускная способность также снижается до 810.72 Mbps, 780.00 Mbps, 730.00

Mbps, и 680.00 Mbps для 1, 2, 4 и 8 потоков. Шифрование UDP вызывает дополнительные потери производительности, особенно при высоких нагрузках. График 2 показывает, что пропускная способность в Docker и TCP оказалась самой низкой: 780.88 Mbps, 750.00 Mbps, 700.00 Mbps, и 650.00 Mbps для 1, 2, 4 и 8 потоков. Это связано с накладными расходами, вызванными изоляцией контейнеров и виртуализацией сетевых интерфейсов. С UDP показатели снизились до 745.58 Mbps, 710.00 Mbps, 650.00 Mbps, и 600.00 Mbps для 1, 2, 4 и 8 потоков. Увеличение нагрузки на систему и сеть в Docker приводит к дополнительным потерям производительности, особенно при многопоточности.

3. Видимость трафика

Из таблицы 1 следует, что без Shadowsocks трафик не шифруется и передается в открытом виде, позволяя с помощью tcpdump легко выявить исходные и целевые адреса, порты и содержимое передаваемых пакетов. Это делает данные уязвимыми для перехвата и анализа. График 3 указывает, что с включенным Shadowsocks весь трафик шифруется, и при попытке захвата пакетов с помощью tcpdump они выглядят как случайные данные. Даже если пакеты будут перехвачены, злоумышленник не сможет прочитать их содержимое без соответствующего ключа дешифрования. Это значительно повышает безопасность и конфиденциальность передаваемых данных.

Графики 3–4 (Рисунок 3,4) показывают, что Ntopng и Bmon показали снижение общего трафика и скорости передачи данных при использовании Shadowsocks и Docker. Для Ntopng общий трафик уменьшился с 102.34 MB до 95.67 MB при включении Shadowsocks и до 88.45 MB при использовании Docker. Из графика 4 видно, что в случае с Bmon средняя скорость передачи данных снизилась с 930.12 Mbps до 820.45 Mbps с Shadowsocks и до 760.34 Mbps в Docker. Эти результаты подтверждают, что использование Shadowsocks и Docker снижает пропускную способность сети

Таким образом, результаты тестирования показывают, что после включения Shadowsocks, мы видим следующие изменения. Наблюдается увеличение времени задержки: это нормальная реакция сети на дополнительную нагрузку, связанную с процессом шифрования. Однако увеличение задержки на 5–15 ms не является критичным для большинства пользовательских приложений. Происходит снижение пропускной способности: это также ожидаемый результат, поскольку шифрование требует вычислительных ресурсов. Особенно значительное снижение наблюдается в тестах на UDP, где отсутствие встроенных механизмов контроля потока делает его более чувствительным к нагрузке. Подводя итоги, использование Shadowsocks повышает безопасность соединения, обеспечивая шифрование данных. Tcpdump показывает, что трафик становится нечитаемым для анализа, что существенно уменьшает риск перехвата конфиденциальной информации.

Заключение

В заключении будут приведены несколько пунктов, каждый из которых будет раскрыт более подробно, первым будет краткое описание проведенного исследования, затем результат проверки гипотез и направления дальнейшего исследования.

Краткий анализ результатов:

В результате анализа полученных значений можно сделать вывод, что при использовании Shadowsocks, сеть испытывает нагрузку: время задержки увеличивается на 5–

15 мс из-за процесса шифрования, пропускная способность также ниже, чем при первоначальных тестированиях. Особенно значительное снижение наблюдается в тестах UDP, где отсутствие встроенных механизмов управления потоком делает его более чувствительным к нагрузке. Время передачи данных соответственно увеличилось в связи с шифрованием данных на клиенте и последующей дешифровкой на клиенте. Однако поскольку тип трафика стал зашифрованным, значительно увеличилась безопасность соединения, несмотря на небольшую задержку, система работает в штатном режиме.

Результат проверки гипотез:

Первая гипотеза о том, что при использовании Shadowsocks будет увеличено время задержки и снижена пропускная способность по сравнению с обычным соединением без использования с, была подтверждена. Вторая гипотеза о том, что при использовании Shadowsocks будет повышена безопасность соединения, также согласуется с результатами исследования. Третья гипотеза о том, что при использовании метода установки Shadowsocks через пакеты или git будет получена более быстрое соединение по сравнению с установкой через Docker, подтвердила правильность предложенной гипотезы.

Направления дальнейшего исследования:

Будущие исследования могут сосредоточиться на сравнении технологии Shadowsocks с другими технологиями шифрования трафика, также можно исследовать возможность оптимизации Shadowsocks для уменьшения задержки и увеличения пропускной способности, так как это важно для реального передачи данных в реальном времени. Другим направлением исследования может стать разработка новых алгоритмов или модификаций Shadowsocks, которая может улучшить его совместимость с различными типами сетей.

Список литературы

1. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование: Практикум. Учебное пособие для вузов / А. Г. Уймин. – Санкт-Петербург: Издательство "Лань", 2024. – 116 с. – (Высшее образование). – ISBN 978-5-507-48647-2. – EDN BZJRIQ.
2. What Is Shadowsocks, and How Does It Work? // How-To-Geek URL: https://www.howtogeek.com/795336/what-is-shadowsocks-and-how-does-it-work/ (дата обращения: 10.12.2024).
3. Shadowsocks Wiki. // GitHub. // URL: https://github.com/shadowsocks/shadowsocks/wiki (дата обращения: 10.12.2024).
4. AEAD Ciphers. // Shadowsocks. // URL: https://shadowsocks.org/doc/aead.html (дата обращения: 10.12.2024).
5. Альт // Российский разработчик операционных систем "Альт" URL: https://www.basealt.ru/alt-workstation (дата обращения: 10.12.2024).
6. Указ Президента Российской Федерации от 30.03.2022 г. № 166// Правительство России. // URL: http://www.kremlin.ru/acts/bank/47688 (дата обращения: 10.12.2024).
7. Новости // Российский разработчик операционных систем "Альт" URL: https://www.basealt.ru/about/news/archive/view/os-mnogo-reestr-odin-10-pravil-kak-vybrat-nadezhnuju-rossiiskuju-operacionnuju-sistemu (дата обращения: 10.12.2024).

8. Главная страница // ALT Linux Wiki URL: https://www.altlinux.org/ (дата обращения: 10.12.2024).

References

1. Uimin, A. G. Basic level demonstration exam. Network and System Administration: A practical course. Textbook for universities / A. G. Uimin. Saint Petersburg: Lan Publishing House, 2024. 116 p. (Higher education). – ISBN 978-5-507-48647-2. – EDN BZJRIQ.
2. What Is Shadowsocks, and How Does It Work? // How-To-Geek URL: https://www.howtogeek.com/795336/what-is-shadowsocks-and-how-does-it-work/ (дата обращения: 10.12.2024).
3. Shadowsocks Wiki. // GitHub. URL: https://github.com/shadowsocks/shadowsocks/wiki (accessed 10.12.2024).
4. AEAD Ciphers. // Shadowsocks. URL: https://shadowsocks.org/doc/aead.html (accessed 10.12.2024).
5. Alt // Russian developer of operating systems "Alt" URL: https://www.basealt.ru/alt-workstation (accessed: 10.12.2024).
6. Decree of the President of the Russian Federation of 30.03.2022 No 166 // Government of Russia. Available at: http://www.kremlin.ru/acts/bank/47688 (accessed: 10.12.2024).
7. News // Russian developer of operating systems "Alt" URL: https://www.basealt.ru/about/news/archive/view/os-mnogo-reestr-odin-10-pravil-kak-vybrat-nadezhnuju-rossiiskuju-operacionnuju-sistemu (accessed 10.12.2024)
8. Main page // ALT Linux Wiki URL: https://www.altlinux.org/ (accessed: 10.12.2024).