Криничев Е.Е., Матюшин А.М. Сравнение графического интерфейса отечественного линукса со стороны безопасности и администрирования // Международный журнал информационных технологий и энергоэффективности. – 2025. – Т. 10 № 2(52) с. 156-–165

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

СРАВНЕНИЕ ГРАФИЧЕСКОГО ИНТЕРФЕЙСА ОТЕЧЕСТВЕННОГО ЛИНУКСА СО СТОРОНЫ БЕЗОПАСНОСТИ И АДМИНИСТРИРОВАНИЯ

[1] **Криничев Е.Е., Матюшин А.М.**
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] egorkrinichev@mail.ru

В статье проведён сравнительный анализ графических оболочек российских дистрибутивов Linux: Astra Linux, REDOS-8, ALT Linux и ROSA с акцентом на безопасность и администрирование. Рассматриваются особенности оболочек MATE, GNOME и FLY, их уязвимости и применимость в коммерческой и научной деятельности.

Ключевые слова: GNOME, MATE, АЛЬТ Linux, ROSA Linux, РЕД ОС, Astra Linux, безопасность, администрирование.

COMPARISON OF THE GRAPHICAL INTERFACE OF DOMESTIC LINUX IN TERMS OF SECURITY AND ADMINISTRATION

[1] **Krinichev E.E., Matyushkin A.M.**
GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: [1] egorkrinichev@mail.ru

The article presents a comparative analysis of the graphical interfaces of Russian Linux distributions: Astra Linux, REDOS-8, ALT Linux, and ROSA, with a focus on security and administration. The study examines the features of MATE, GNOME, and FLY interfaces, their vulnerabilities, and applicability in commercial and scientific activities.

Keywords: GNOME, MATE, ALT Linux, ROSA Linux, RED OS, Astra Linux, security, administration.

Введение

В современном цифровом мире, где информация становится ключевым ресурсом, администрирование и обеспечение безопасности информационных систем приобретают первостепенное значение. Для достижения суверенитета и независимости в IT-сфере разработка отечественного программного обеспечения, включая операционные системы на основе Linux, играет важную роль.

Наше исследование направлено на изучение возможностей администрирования и безопасности данных систем. Особое внимание мы уделяем сильным и слабым сторонам различных графических оболочек, а также анализу ранее выявленных уязвимостей, чтобы найти оптимальные решения для конкретных задач.

Для начала изучим какие графические оболочки предоставляют нам следующие версии наших ОС:

Таблица 1 – Версии ОС.

ОС версия	Ядро версия	Графика версия	Количество пакетов в графике
ALT рабочая станция версии 10.2	6.1.79	Mate v: 1.26.1	1955
ROSA.FRESH.GNOME версии 12.5.1	6.6.47	Gnome v:42.9	2625
RESOS-8 от 18.02.2024	6.6.51-1	Mate v: 1.26.0	1991
Astra linux версии 1.8 от 27.06.2024	6.1.9	Fly v: 1.21.1	2208

Для этого используем утилиту *inxi.*

```
user@matyushin ~/Рабочий стол $ inxi -F
System:
  Host: matyushin Kernel: 6.6.27-generic-3rosa2021.1-x86_64 arch: x86_64
    bits: 64 Desktop: GNOME v: 42.9 Distro: ROSA Fresh Desktop 12.5.1 release
    2021.1 for x86_64
```

Рисунок 1 – «ROSA»

```
[root@host-15 ~]# inxi -F
System:
  Host: host-15 Kernel: 6.1.79-un-def-alt1 arch: x86_64 bits: 64 Desktop: MATE
    v: 1.26.1 Distro: ALT Workstation 10.2
```

Рисунок 2 – «ALT»

```
  Host: localhost Kernel: 6.6.6-1.red80.x86_64 x86_64 bits: 64
  Desktop: MATE 1.26.0 Distro: RED OS release (8.0) DESKTOP
```

Рисунок 3 – «REDOS»

Для ОС ASTRA Linux утилита inxi отсутствует, но графическая оболочка пишется при установлении ОС:

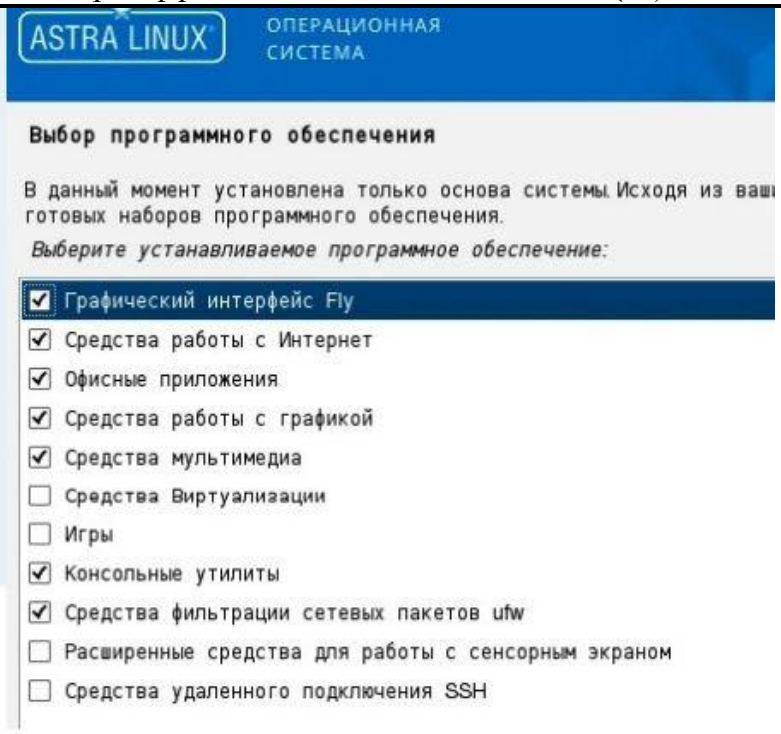

Рисунок 4 – «ASTRA Linux»

У ОС ASTRA Linux своя графическая оболочка «FLY», что отличает ее от своих конкурентов, которые используют стандартные решения в данном вопросе GNOME v 42.9 и MATE v 1.26.0/1.26.1.[1]

Графические окружения, такие как MATE и GNOME, играют важную роль в процессе администрирования. MATE — это легковесное окружение, которое характеризуется стабильностью и низкими системными требованиями. Оно идеально подходит для задач, где важна скорость работы и минимальное потребление ресурсов. GNOME, напротив, предлагает современный интерфейс с широкими функциональными возможностями, включая поддержку множества расширений. [2] Однако он требует больше ресурсов и может быть избыточным для задач с минимальными интерфейсными требованиями, таких как киоск-режим. Для администрирования GNOME будет полезен в крупных инфраструктурах с требованием удобной визуализации, а MATE станет отличным выбором для маломощных систем.

Графические оболочки GNOME и MATE строятся на архитектурах, которые тесно связаны с базовыми компонентами Linux, такими как D-Bus, X11 или Wayland. Их безопасность напрямую зависит от надежности этих базовых технологий. Именно безопасность этих компонентов часто становится решающим фактором в выборе графической среды. Рассмотрим их особенности и проблемы безопасности.[3]

D-Bus (Desktop Bus) — это система сообщений, которая позволяет приложениям общаться друг с другом или с системными службами. Она играет ключевую роль в обоих графических окружениях, GNOME и MATE. В GNOME и MATE D-Bus используется для управления сессиями, обмена данными между приложениями и вызова системных процессов. [4] Например, через D-Bus передаются события блокировки экрана, открытия файлов и уведомления от системы.

X11 (или X.Org Server) — это устаревший, но до сих пор широко используемый протокол для графического вывода. Он является основой MATE и некоторых версий GNOME. Главная проблема X11 — отсутствие изоляции. Приложения, работающие в одном X-сервере, имеют доступ к общим данным. Это делает X11 уязвимым к атакам, таким как перехват паролей или данных из других окон. MATE полностью полагается на X11, так как его архитектура ориентирована на стабильность и совместимость. GNOME постепенно отходит от X11 в пользу Wayland, но поддержка X11 все еще сохраняется для совместимости.[5]

Wayland — это современный протокол для графического вывода, который был создан как замена X11 с акцентом на безопасность и производительность. GNOME активно использует Wayland, начиная с версий 3.22 и выше, в то время как MATE только начинает внедрять его поддержку. Главная особенность Wayland — изоляция оконных процессов. Это означает, что одно приложение не может получить доступ к содержимому окна другого приложения или его событиям. Такой подход полностью устраняет класс атак, характерных для X11. Уязвимости могут возникать на уровне реализации (например, в композиторах, таких как Mutter в GNOME). Однако риск подобных атак значительно ниже из-за более строгой архитектуры.

С точки зрения администрирования рассмотрим возможности ОС для реализации режима «киоск», который имеет популярность при администрировании распределенных информационных систем.[6]

Режим киоска (от англ. "kiosk mode") в Linux — это специализированный режим работы операционной системы, предназначенный для ограничения доступа пользователя к определённым функциям системы и предоставления возможности выполнения только заранее определённых задач. Этот режим широко используется для обеспечения безопасности и стабильности работы устройств, предоставляющих публичный доступ или работающих в узкоспециализированных сценариях.

ALT Linux представляет собой систему с минималистичным подходом, что обеспечивает легкость её развертывания. [7] Инструмент alterator-kiosk позволяет быстро настроить режим киоска, предоставляя пользователю строго ограниченный функционал. Благодаря поддержке SELinux и AppArmor обеспечивается высокий уровень безопасности. Однако, ALT Linux требует большего уровня подготовки от администратора при настройке нестандартных сценариев и практически не предлагает визуальных инструментов, что может осложнить работу новичков. Тем не менее, возможность кастомизации интерфейса (включая использование облегчённых оконных менеджеров) и централизованного управления через образы или сети делает эту систему удобной для небольших инфраструктур.

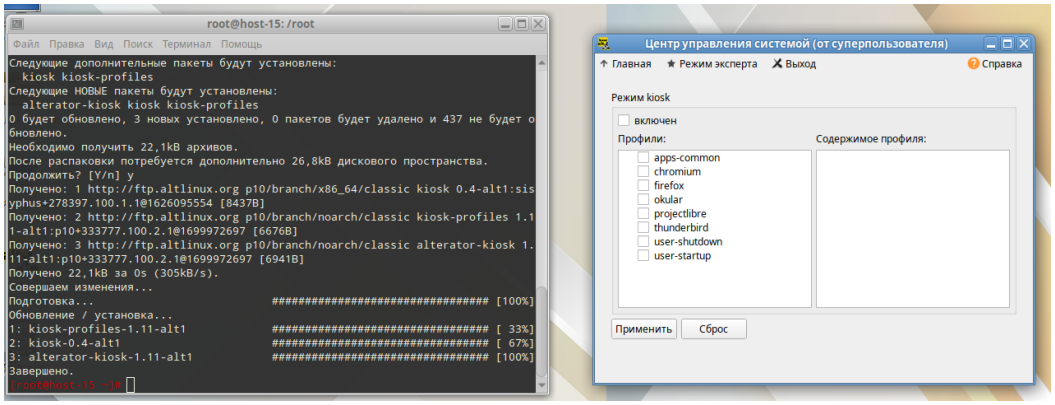

Рисунок 5 – «ALT киоск»

REDOS-8 отличается строгим соблюдением требований сертифицированной безопасности, что делает её выбором номер один для госструктур, банков и образовательных учреждений. [8] Она поддерживает мандатный контроль доступа, ограничивающий несанкционированные действия пользователей. Режим киоска на базе REDOS-8 обладает полезными функциями, такими как автоматическое скрытие панели, работа приложений в песочнице и сброс данных после завершения сессии. Однако интерфейс настройки преимущественно консольный, что усложняет работу администраторов без соответствующей подготовки. Тем не менее, REDOS-8 превосходит большинство систем по масштабу поддерживаемых сценариев и гибкости ограничений.

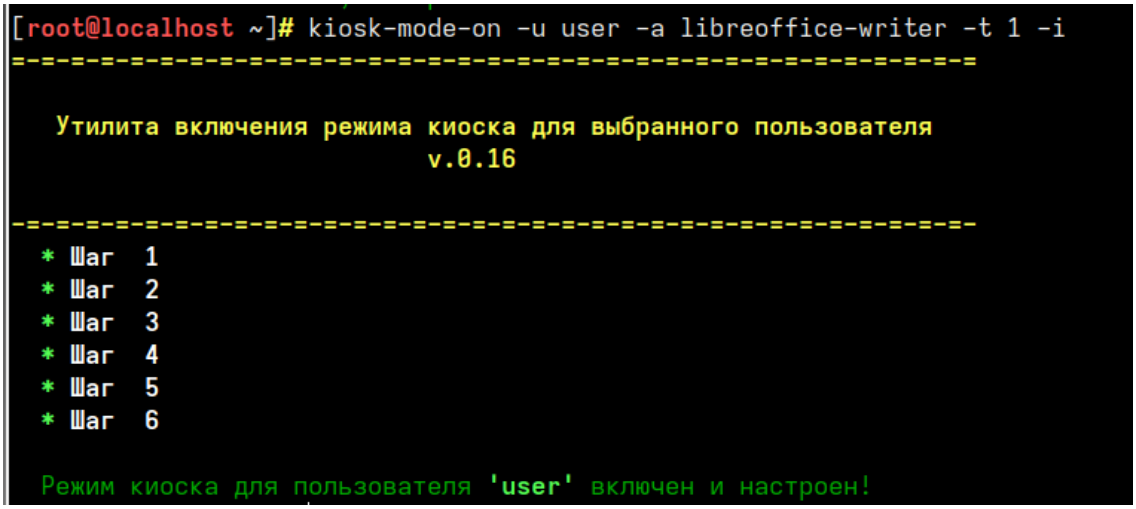

Рисунок 6 – «REDOS-8 киоск»

Astra Linux обеспечивает оптимальный баланс между удобством и безопасностью. Предоставляя графические интерфейсы для настройки и инструменты мандатного контроля, Astra Linux упрощает администрирование, даже в условиях высоких требований к защите данных. Поддержка журналирования и восстановление неизменяемой файловой системы делают эту ОС привлекательной для организаций, нуждающихся в прозрачности действий пользователей. [9] Однако сложность настройки продвинутых политик безопасности может потребовать от администратора дополнительных знаний. Astra Linux подходит для крупных инфраструктур с высоким уровнем стандартизации.

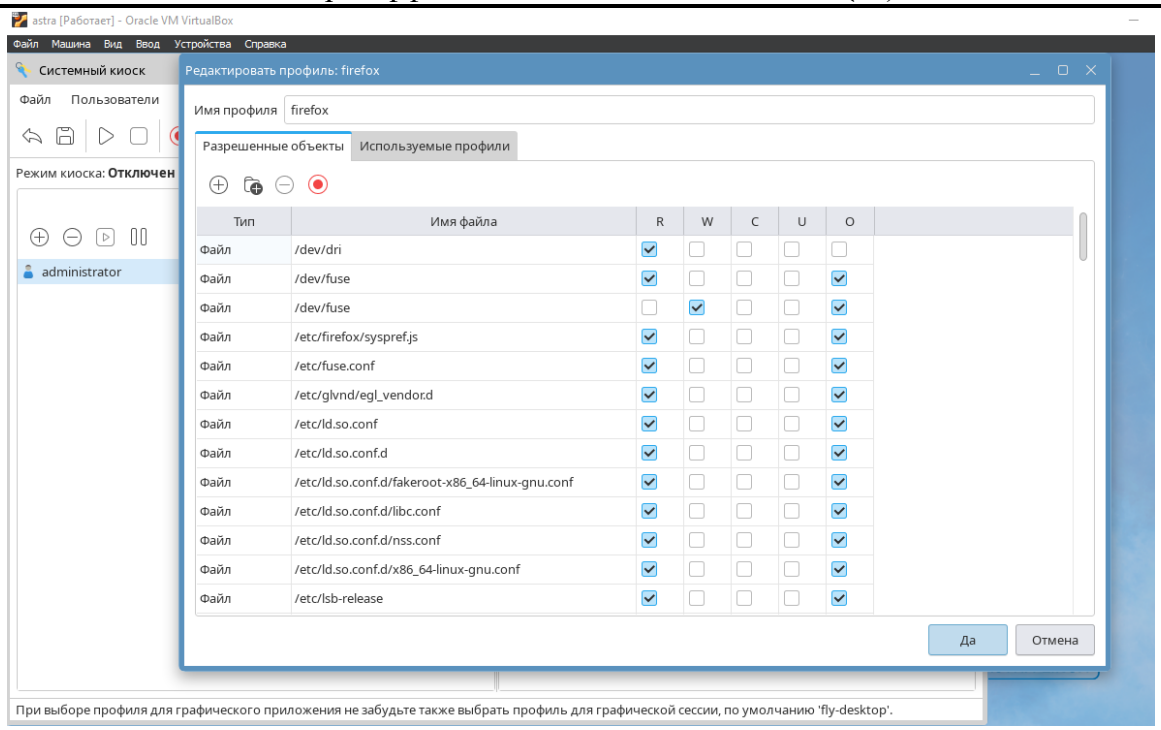

Рисунок 7 – «ASTRA Linux киоск»

У операционной системы ROSA нету утилиты, которая реализовывала бы работы киоска, поэтому в вопросе администрирование она изначально выглядит слабее конкурентов. [10] Но тем не менее можно использовать стандартный сервисы для администрирования, например:

- Sudo - программа для системного администрирования UNIX-систем, позволяющая делегировать те или иные привилегированные ресурсы пользователям с ведением протокола работы.
- OpenLDAP - используется для управления учётными записями и контроля доступа в сетях
- Kerberos - поддержка централизованной аутентификации для корпоративных сетей.
- Wine — представляет собой слой совместимости, позволяющий запускать Windows-приложения на других операционных системах, таких как Linux, macOS и BSD.

Данные инструменты также подходят и для остальных ОС.

Мы ознакомились с возможностями каждой ОС и сделали таблицу, где от рейтинговали их по выбранным параметрам.

Таблица 1 - Сравнение ОС в аспекте администрирования

Параметры оценки	Astra Linux	Red OS	ALT Linux	ROSA
Уровень безопасности	1	1	3	4
Простота настройки	1	3	2	4
Масштабируемость	1	2	3	4
Централизованное управление	1	2	3	4
Кастомизация интерфейса	1	3	2	4
Сумма баллов	5	**11**	**13**	20

Таким образом, Astra Linux, по администрированию, будет лучшим вариантом. Второе и третье место с минимальной разницей занимают REDOS-8 и ALT Linux. И худший вариант в данном аспекте будет ROSA.

Теперь давайте изучим данные графические оболочки операционных систем с точки зрения безопасности, для этого нам нужно провести анализ зарегистрированных CVE связанных с GNOME и MATE. В данном вопросе мы не будем рассматривать «FLY» от ASTRA по причине, того, что в открытых базах данных на ней не было зарегистрировано CVE, с одной стороны это может говорить о отличной системе защиты, с другой - не изученности данного вопроса, как со стороны атаки, так и со стороны защиты.

На основе анализа открытых баз данных (NVD, MITRE CVE) было выявлено:

GNOME:

Количество зарегистрированных уязвимостей с упоминанием GNOME на ресурсе cve.mitre.org: 259 CVE.

Типичные проблемы:

- Переполнение буфера (например, CVE-2024-36472).
- Утечка данных (CVE-2021-3800).
- Уязвимости в библиотеке GdkPixbuf (CVE-2022-48622).

MATE:

- Количество зарегистрированных уязвимостей с упоминанием MATE на ресурсе cve.mitre.org: 126 CVE.
- Типичные проблемы:
- Уязвимости в обработке пользовательского ввода (например, CVE-2018-20681).
- Проблемы в компонентах, таких как mate-screensaver.
- Пример: CVE-2018-20681 — проблема с mate-screensaver, которая могла быть использована для обхода блокировки экрана.

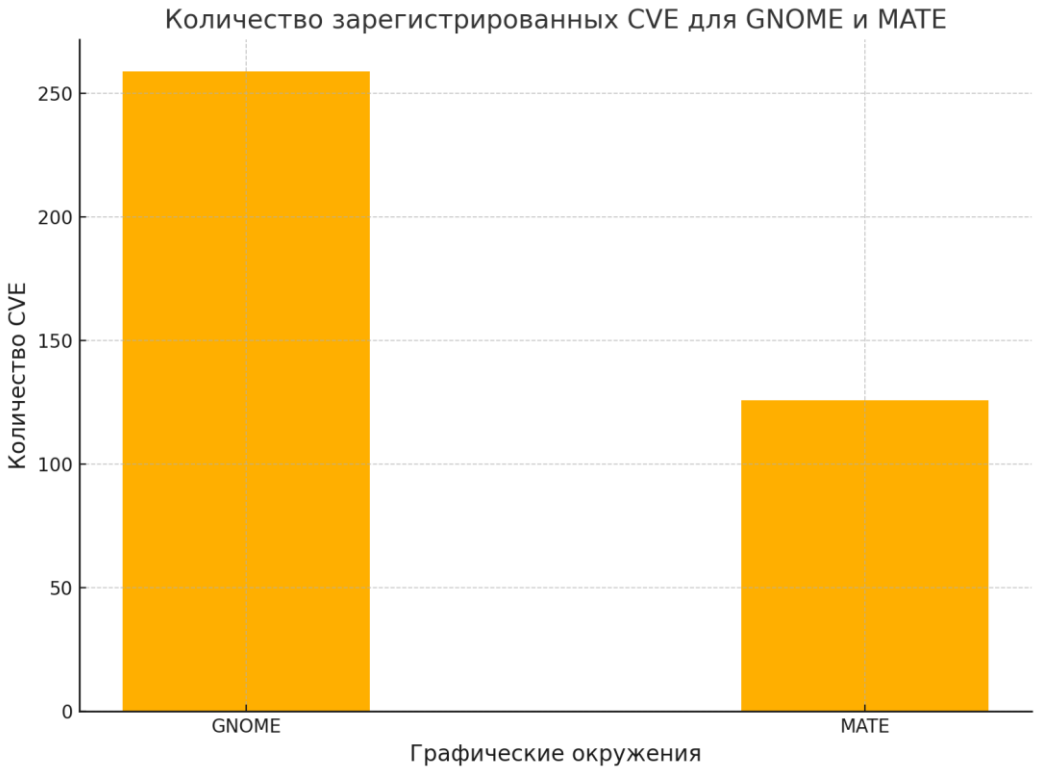

Рисунок 8 – Количественное сравнение GNOME/MATE

Сравнительный анализ безопасности

1) Сложность системы:

- GNOME:
  - Плюсы: более современный и функциональный интерфейс, поддержка новейших технологий.
  - Минусы: сложность архитектуры увеличивает вероятность уязвимостей.
- MATE:
  - Плюсы: легковесная и стабильная архитектура снижает риск появления новых уязвимостей.
  - Минусы: ограниченная функциональность может быть недостаточной для современных задач.

2) Активность разработки:

- GNOME: частые обновления приводят к быстрому обнаружению и исправлению уязвимостей.
- MATE: менее частые обновления, но стабильный код минимизирует риск новых проблем.

3) Подверженность атакам:

- GNOME: чаще становится целью атак из-за своей популярности.
- MATE: меньшая распространённость снижает риск целенаправленных атак.

MATE оказывается более безопасной благодаря своей простой архитектуре и меньшему числу уязвимостей. Однако GNOME предлагает значительно более широкий набор функций и активно обновляется, что позволяет быстро устранять обнаруженные проблемы. Выбор между этими оболочками зависит от предпочтений пользователя: если важнее безопасность и стабильность — MATE; если функциональность и современные возможности — GNOME.

Разработчикам и администраторам рекомендуется регулярно обновлять систему, следить за отчетами об уязвимостях и использовать дополнительные меры защиты, такие как шифрование и изоляция приложений.

Заключение

На основе проведённого анализа выявлено, что Astra Linux является наиболее сбалансированным решением для администрирования и обеспечения безопасности. Её преимущества включают высокую степень защиты данных, удобство настройки и развитую систему централизованного управления. Это делает Astra Linux оптимальным выбором для крупных инфраструктур.

REDOS-8 выделяется строгими стандартами безопасности, что делает её подходящей для госструктур и финансовых учреждений, однако консольный подход к настройке усложняет использование для менее подготовленных администраторов. ALT Linux, благодаря своей простоте и минималистичному подходу, лучше всего подходит для небольших организаций, где важна лёгкость развертывания. ROSA остаётся жизнеспособным вариантом для менее критичных задач, несмотря на отсутствие встроенного киоск-режима.

Выбор графической оболочки также зависит от целей: MATE (ALT, REDOS-8) показывает лучшую стабильность и меньшую уязвимость, тогда как GNOME (ROSA) предоставляет более широкий функционал, но требует больше ресурсов и имеет больше зарегистрированных уязвимостей.

Таким образом, выбор системы должен основываться на специфике задач и требованиях к безопасности. В дальнейшем необходимо учитывать динамику обновлений, количество выявляемых уязвимостей и специфические сценарии эксплуатации.

Список литературы

1. Уймин, А. Г. Оценка безопасности wine с использованием методологии stride: математическая модель / А. Г. Уймин, И. М. Морозов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2023. – № 6-2. – С. 164-170. – DOI 10.37882/2223-2982.2023.6-2.40. – EDN HYCKNP. (дата обращения: 11.12.2024).
2. Wayland Architecture and Security // Wayland URL: https://wayland.freedesktop.org/ (дата обращения: 01.12.2024).
3. GNOME Wayland Transition Guide // Gnome URL: https://wiki.gnome.org/Initiatives/Wayland (дата обращения: 01.12.2024).
4. MATE Desktop Documentation // MATE Desktop Environment URL: https://mate-desktop.org/ (дата обращения: 03.12.2024).
5. Получение технической информации о ПК // РЕДОС URL: https://redos.red-soft.ru/base/redos-7_3/7_3-equipment/7_3-test-soft/7_3-hardware-info/?nocache=1734893761767 (дата обращения: 02.12.2024).
6. Управление пакетами // РЕДОС URL: https://redos.red-soft.ru/base/redos-7_3/7_3-base-consept/7_3-sys-dnf/7_3-gen-info-dnf/7_3-manage-package/?nocache=1734893816094 (дата обращения: 02.12.2024).
7. Как устроена графика в Linux: обзор различных сред оформления рабочего стола // Habr URL: https://habr.com/ru/companies/lanit/articles/516330/ (дата обращения: 05.12.2024).
8. Открытая база данных CVE // CVE URL: https://cve.mitre.org/ (дата обращения: 30.11.2024).
9. Комплексная аналитика уязвимостей // База данных CVE URL: https://vulners.com/ (дата обращения: 30.11.2024).
10. National Vulnerability Database // NIST URL: https://nvd.nist.gov/ (дата обращения: 30.11.2024).

References

1. Uimin, A. G. Wine safety assessment using stride methodology: a mathematical model / A. G. Uimin, I. M. Morozov // Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. - 2023. – No. 6-2. – pp. 164-170. – DOI 10.37882/2223-2982.2023.6-2.40. – EDN HYCKNP. (date of request: 11.12.2024).
2. Wayland Architecture and Security // Wayland URL: https://wayland.freedesktop.org / (date of access: 12/01/2024).
3. GNOME Wayland Transition Guide // Gnome URL: https://wiki.gnome.org/Initiatives/Wayland (accessed: 12/01/2024).

4. MATE Desktop Documentation // MATE Desktop Environment URL: https://mate-desktop.org / (date of access: 12/03/2024).
5. Getting technical information about the PC // REDOS URL: https://redos.red-soft.ru/base/redos-7_3/7_3-equipment/7_3-test-soft/7_3-hardware-info/?nocache=1734893761767 (date of request: 02.12.2024).
6. Package Management // REDOS URL: https://redos.red-soft.ru/base/redos-7_3/7_3-base-consept/7_3-sys-dnf/7_3-gen-info-dnf/7_3-manage-package/?nocache=1734893816094 (accessed: 12/02/2024).
7. How graphics work in Linux: an overview of various desktop design environments // Habr URL: https://habr.com/ru/companies/lanit/articles/516330 / (accessed: 05.12.2024).
8. Open CVE database // CVE URL: https://cve.mitre.org / (date accessed: 11/30/2024).
9. Comprehensive Vulnerability Analytics // CVE database URL: https://vulners.com / (date of access: 11/30/2024).
10. National Vulnerability Database // NIST URL: https://nvd.nist.gov / (date of access: 11/30/2024).