Филатов Р. А., Мордвинова А.Ю. Архитектурные принципы защиты операционных систем LINUX: рекомендации федерального регулятора// Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 6(68) Ч.1 с. 101–104

Международный журнал информационных технологий и энергоэффективности

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



УДК 004.056:004.7.056

АРХИТЕКТУРНЫЕ ПРИНЦИПЫ ЗАЩИТЫ ОПЕРАЦИОННЫХ СИСТЕМ LINUX: РЕКОМЕНДАЦИИ ФЕДЕРАЛЬНОГО РЕГУЛЯТОРА

Филатов Р. А., [1]**Мордвинова А.Ю**.
ФГАОУ ВО "СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ", Севастополь, Россия (299053, город Севастополь, Университетская ул., зд. 33), e-mail: [1] aumordvinova@mail.sevsu.ru

В статье рассматривается комплексный подход к конфигурированию операционных систем семейства Linux в соответствии с методическими рекомендациями Федеральной службы по техническому и экспортному контролю (ФСТЭК) России.

Ключевые слова: безопасность Linux, критическая информационная инфраструктура, методические рекомендации ФСТЭК, управление доступом, безопасная конфигурация ОС.

ARCHITECTURAL PRINCIPLES FOR LINUX OPERATING SYSTEM SECURITY: FEDERAL REGULATOR RECOMMENDATIONS

Filatov R. A., [1]**Mordvinova A. Yu.**
SEVASTOPOL STATE UNIVERSITY, Sevastopol, Russia (299053, Sevastopol, Universitetskaya st., 33), e-mail: [1] aumordvinova@mail.sevsu.ru

This article examines a comprehensive approach to configuring Linux operating systems in accordance with the guidelines of the Federal Service for Technical and Export Control (FSTEC) of Russia.

Keywords: Linux security, critical information infrastructure, FSTEC guidelines, access control, secure OS configuration

Введение

В условиях цифровизации государственной инфраструктуры и объектов критической информационной защиты перед IT-специалистами стоит задача обеспечения надёжной безопасности операционных систем семейства Linux. Федеральная служба по техническому и экспортному контролю разработала методические рекомендации, определяющие комплексный подход к конфигурированию ОС на основе ядра Linux в государственных информационных системах и объектах критической инфраструктуры РФ до момента полного перехода на сертифицированные отечественные решения. Переход к открытым программным решениям в государственном секторе обусловлен не только требованиями технологического суверенитета, но и необходимостью обеспечения прозрачности кода и гибкости настройки защитных механизмов. В связи с этим администраторам информационных систем необходимо внедрять принципы защиты по умолчанию и минимально необходимых привилегий, что напрямую коррелирует с базовыми требованиями регуляторов и формирует основу для построения эшелонированной обороны.

Основная часть

Фундамент безопасности любой операционной системы закладывается на уровне управления учётными записями. Первоочередное внимание должно уделяться исключению использования учётных записей с отсутствующими парольными защитами. Каждому активному пользователю системы необходимо установить уникальный пароль или заблокировать учётную запись через редактирование параметров файла /etc/shadow. Помимо базового блокирования пустых паролей, рекомендуется настроить политики сложности, минимальной длины и срока действия учётных данных. [1] Для этого используются модули PAM, такие как pam_pwquality, позволяющие задавать требования к наличию символов разных регистров и цифр, а также ограничивать повторное использование предыдущих паролей. Дополнительно целесообразно внедрить автоматическую временную блокировку учётных записей после заданного числа неудачных попыток входа, что эффективно противодействует автоматизированным атакам подбора учётных данных.

Критически важным является отключение возможности удалённого входа суперпользователя через SSH-протокол посредством установки параметра PermitRootLogin no в конфигурационном файле /etc/ssh/sshd_config. [2] Такой подход минимизирует риск несанкционированного доступа на уровне наивысших привилегий. В дополнение к запрету прямого входа от имени root рекомендуется перевести аутентификацию в SSH на использование криптографических ключей, отключив вход по паролю директивой PasswordAuthentication no. Изменение стандартного порта службы и применение средств динамической фильтрации, таких как Fail2Ban или встроенные механизмы iptables/nftables, создают дополнительный рубеж обороны, затрудняя автоматизированное сканирование портов и подбор учётных записей злоумышленниками.

Механизмы получения повышенных привилегий требуют строгого контроля. Команда su должна быть ограничена только для определённого круга пользователей посредством добавления соответствующей строки в файл PAM-конфигурации (/etc/pam.d/su). Список авторизованных пользователей указывается в группе wheel в файле /etc/group. Аналогично, доступ к команде sudo должен быть пересмотрен и ограничен через редактирование файла /etc/sudoers, где администратор может явно указать, какие пользователи могут выполнять какие команды с повышенными привилегиями. Особое значение приобретает обязательное журналирование всех действий, выполняемых с повышенными привилегиями. Настройка подсистемы auditd позволяет фиксировать не только успешные и неудачные попытки использования sudo или su, но и отслеживать изменения в критических конфигурационных файлах, запуск нестандартных процессов и обращения к защищённым системным ресурсам. Интеграция журналов с централизованными SIEM-платформами обеспечивает возможность оперативного реагирования на инциденты и формирования отчётности для регуляторных проверок.[3]

Правильная настройка прав доступа представляет собой второй уровень защиты. Файлы, содержащие информацию об учётных записях (/etc/passwd, /etc/group), должны иметь права 644, что позволяет всем пользователям их читать, но модифицировать могут только владельцы. В то же время, файлы хранилищ хешей паролей (/etc/shadow в системах GNU/Linux, Solaris, HP-UX или /etc/security/passwd в AIX) должны быть доступны только администраторам системы с правами 700 или эквивалентными (go-rwx).

Все исполняемые файлы, запущенные в текущий момент, и соответствующие им системные библиотеки не должны быть доступны для записи непривилегированным пользователям. Это достигается через команду вида chmod go-w /путь/к/файлу с последующей проверкой прав доступа на родительские директории. Особое внимание требуется к стартовым скриптам системы в директориях /etc/rc#.d и systemd-модулям (.service-файлы), права доступа к которым должны быть установлены посредством chmod o-w.

Файлы заданий планировщика cron (как системные в /etc/crontab, /etc/cron.d, /etc/cron.hourly, так и пользовательские) должны быть защищены от записи с помощью chmod go-wx. Критически важным является защита SUID/SGID-приложений: все такие приложения должны быть подвергнуты аудиту, и с тех из них, которые не являются необходимыми, должны быть сняты соответствующие биты. [4] Домашние директории пользователей требуют установки прав 700, а файлы истории команд и конфигурации оболочки (.bash_history, .bashrc, .profile) должны быть недоступны для просмотра и модификации другими пользователями. На уровне файловой системы целесообразно применять дополнительные параметры монтирования, такие как noexec, nosuid и nodev для разделов, содержащих пользовательские данные или временные файлы. Это предотвращает запуск произвольного кода и эксплуатацию уязвимостей через специальные биты в непредназначенных для этого директориях. Регулярное обновление ядра и пакетного состава, а также автоматизированный аудит конфигураций с использованием специализированных скриптов или инструментов соответствия стандартам CIS Benchmarks, позволяют своевременно выявлять отклонения от безопасного базового образа системы и закрывать уязвимости до их использования злоумышленниками.

Заключение

Безопасность операционных систем Linux требует комплексного подхода, объединяющего правильную конфигурацию подсистемы управления доступом, защиту критических файловых ресурсов, оптимизацию параметров ядра для минимизации вектора атак, изоляцию компонентов и активный мониторинг. Важно подчеркнуть, что единовременная настройка защитных механизмов не гарантирует долгосрочной устойчивости инфраструктуры. Безопасность Linux-систем в критической среде требует непрерывного цикла оценки, обновления политик и адаптации к изменяющемуся ландшафту угроз. Проведение периодических внутренних аудитов, тестирование на проникновение и обучение административного персонала актуальным практикам безопасной эксплуатации становятся неотъемлемыми элементами жизненного цикла защищённой системы. Методические рекомендации ФСТЭК, разработанные для государственных информационных систем, представляют собой проверенную архитектурную схему, обеспечивающую надёжную защиту от разнообразных классов атак при условии их полного и правильного внедрения. Последовательное внедрение описанных мер позволяет значительно повысить устойчивость Linux-систем к современным угрозам информационной безопасности.

Список литературы

1. Методический документ от 25 декабря 2022 г. // ФСТЭК России : сайт. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-25-dekabrya-2022-g (дата обращения: 17.04.2026)

2. Карцан И.Н., Мордвинова А.Ю. Система управления информационными рисками. В сборнике: Вопросы контроля хозяйственной деятельности и финансового аудита, национальной безопасности, системного анализа и управления. Материалы VII Всероссийской научно-практической конференции. Москва, 2022. С. 141-146.
3. Мордвинова А.Ю., Нуриев С.А. Исследование уязвимостей и угроз безопасности стандарта IEEE 802.11. Современные инновации, системы и технологии. 2023. Т. 3. № 3. С. 117-131.
4. Мордвинова А.Ю., Жуков А.О., Аверьянов В.С., Карцан И.Н. Нейросетевая обработка информации в социокиберфизичеких системах. Информационные и телекоммуникационные технологии. 2021. № 52. С. 8-12.

References

1. Methodological document of December 25, 2022 // FSTEC of Russia: website. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-25-dekabrya-2022-g (accessed: April 17, 2026)
2. Kartsan I.N., Mordvinova A.Yu. Information Risk Management System. In the collection: Issues of Control over Economic Activities and Financial Audit, National Security, Systems Analysis and Management. Proceedings of the VII All-Russian Scientific and Practical Conference. Moscow, 2022. pp. 141-146.
3. Mordvinova A.Yu., Nuriyev S.A. Study of Vulnerabilities and Security Threats of the IEEE 802.11 Standard. Modern Innovations, Systems, and Technologies. 2023. Vol. 3. No. 3. pp. 117-131.
4. Mordvinova A.Yu., Zhukov A.O., Averyanov V.S., Kartsan I.N. Neural Network Information Processing in Sociocyber-Physical Systems. Information and Telecommunication Technologies. 2021. No. 52. pp. 8-12.