УДК 004.451.9

Абиев Вадим Тагирович, специалист, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург

Антуфьев Илья Максимович, специалист, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург

Титов Максим Андреевич, специалист, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург

АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОТЕЧЕСТВЕННЫХ LINUX-ОПЕРАЦИОННЫХ СИСТЕМ

Аннотация

В условиях форсированного импортозамещения программного обеспечения и возрастающего количества кибератак на критическую информационную инфраструктуру (КИИ) Российской Федерации выбор защищенной операционной системы становится стратегической задачей. В данной статье проведен комплексный анализ подходов к обеспечению информационной безопасности в ведущих отечественных дистрибутивах: Astra Linux Special Edition, РЕД ОС и ОС «Альт 8 СП». С применением методов структурно-функционального анализа и декомпозиции архитектурных компонентов исследованы реализации мандатного и дискреционного управления доступом, контроля целостности и изоляции процессов. Разработана авторская сравнительная матрица средств защиты информации данных ОС с учетом требований ФСТЭК России. Сделаны выводы о применимости конкретных архитектурных моделей (Белла-

ЛаПадулы, Биба, Type Enforcement) в зависимости от модели нарушителя и класса защищенности инфраструктуры.

Annotation

In the context of accelerated import substitution of software and an increasing number of cyber attacks on the critical information infrastructure (CII) of the Russian Federation, choosing a secure operating system is becoming a strategic task. This article provides a comprehensive analysis of approaches to ensuring information security in leading domestic distributions: Astra Linux Special Edition, RED OS and Alt 8 SP OS. Using methods of structural and functional analysis and decomposition of architectural components, the implementation of mandatory and discretionary access control, integrity control and isolation of processes is investigated. An author's comparative matrix of OS data protection tools has been developed, taking into account the requirements of the FSTEC of Russia. Conclusions are drawn about the applicability of specific architectural models (Bell-LaPadula, Biba, Type Enforcement) depending on the intruder's model and the security class of the infrastructure.

Keywords: information security, operating systems, Linux kernel, mandatory access control, Bell-LaPadula model, Type Enforcement, Astra Linux, RED OS, Alt OS.

Ключевые слова: информационная безопасность, операционные системы, ядро Linux, мандатное управление доступом, модель Белла-ЛаПадулы, Type Enforcement, Astra Linux, РЕД ОС, ОС Альт.

Keywords: information security, operating systems, Linux kernel, mandatory access control, Bell-LaPadula model, Type Enforcement, Astra Linux, RED OS, Alt OS.

1. Введение

На фоне геополитических изменений и ухода с российского рынка

крупнейших зарубежных вендоров программного обеспечения обеспечение технологического суверенитета стало одной из приоритетных задач национальной безопасности [3]. В соответствии с Федеральным законом № 187-ФЗ «О безопасности критической информационной инфраструктуры» [4], государственные структуры и субъекты КИИ обязаны осуществить переход на доверенные отечественные решения.
Фундаментом любой IT-инфраструктуры является операционная система (ОС). Большинство сертифицированных отечественных ОС базируются на открытом ядре Linux. Однако стандартных механизмов безопасности Linux (таких как классическая дискреционная модель прав доступа DAC) недостаточно для противодействия современным целенаправленным атакам (APT) и выполнения строгих требований регуляторов. Это вынуждает отечественных разработчиков глубоко модифицировать архитектуру ОС, интегрируя в ядро собственные подсистемы защиты.
Целью данного исследования является систематизация и оценка эффективности встроенных механизмов безопасности наиболее распространенных отечественных Linux-ориентированных операционных систем. **Методологической базой** исследования послужили методы сравнительного и структурно-функционального анализа, декомпозиция архитектурных компонентов подсистем безопасности, а также метод экспертной оценки соответствия встроенных СЗИ актуальным профилям защиты ФСТЭК России.

2. Теоретическая база: векторы угроз и требования регулятора

Современная операционная система подвергается множеству угроз, среди которых критическими являются: несанкционированный доступ к конфиденциальным данным, повышение привилегий до уровня суперпользователя (root) через эксплуатацию уязвимостей (0-day) и исполнение несанкционированного программного кода.

Для нейтрализации данных угроз ФСТЭК России разделяет требования к ОС на две фундаментальные категории [5]:

1. **Уровни доверия (УД)** (с 6-го по 1-й) — регламентируют безопасность процесса разработки, тестирование на уязвимости и отсутствие недекларированных возможностей (НДВ).
2. **Классы защиты ОС** (типа «А» для рабочих станций и серверов) — регламентируют наличие в ОС конкретных встроенных механизмов безопасности (идентификация, мандатное управление доступом, очистка памяти, контроль целостности).

В зависимости от выбора теоретических моделей (MLS, TE, RBAC) и глубины их интеграции в ядро, разработчики формируют уникальную архитектуру безопасности конкретного дистрибутива.

3. Архитектурный анализ механизмов безопасности

Для исследования были выбраны три операционные системы, занимающие лидирующие позиции в реестре отечественного ПО: Astra Linux Special Edition, РЕД ОС и ОС «Альт 8 СП».

3.1. Astra Linux Special Edition (ГК «Астра»)

ОС Astra Linux Special Edition изначально разрабатывалась для нужд силовых ведомств. Главной архитектурной особенностью системы является отказ от использования модуля SELinux, чья реализация многоуровневой безопасности (MLS) считается избыточно сложной в администрировании, в пользу собственной подсистемы Parsec, интегрированной непосредственно в ядро. Теоретической базой мандатного управления доступом (МАС) в Parsec выступает классическая математическая **модель Белла-ЛаПадулы**, обеспечивающая строгую конфиденциальность: субъекту запрещается чтение данных с более высоким уровнем секретности («чтение вверх») и запись на более низкий («запись вниз»).
Однако ключевым нововведением системы является реализация мандатного

контроля целостности (МКЦ) на базе **модели Биба** [6, с. 45-50]. Этот механизм жестко изолирует системные процессы от пользовательских, запрещая процессам с высоким уровнем целостности (система) читать данные от процессов с низким уровнем (пользователь), что нивелирует риски внедрения вредоносного кода. Дополняет эту архитектуру механизм «Замкнутой программной среды» (ЗПС), аппаратно блокирующий выполнение ELF-файлов без доверенной криптографической подписи.

3.2. РЕД ОС (ООО «РЕД СОФТ»)

Архитектура безопасности РЕД ОС строится на классических компонентах Enterprise-сегмента Linux. Центральным элементом управления доступом является модуль SELinux, работающий в режиме принудительного исполнения (Enforcing).

В отличие от иерархических меток Parsec, SELinux в РЕД ОС опирается на механизм **принудительного присвоения типов (Type Enforcement, TE)** [7]. Каждому процессу (домену) и файлу (типу) назначается контекст безопасности, а их взаимодействие гранулярно описывается разрешающими правилами. Ролевая модель (RBAC) в данном случае выступает лишь надстройкой для привязки пользователей к доменам. Такой подход делает систему легко адаптируемой для администраторов, привыкших к мировым стандартам, однако требует кропотливой настройки политик при внедрении нестандартного прикладного ПО. Контроль программной среды дополнительно обеспечивается демоном fapolicyd на основе белых списков.

3.3. ОС «Альт 8 СП» (ООО «Базальт СПО»)

ОС семейства «Альт» имеют фундаментальное отличие от многих других российских дистрибутивов — они собираются на базе собственной независимой инфраструктуры разработки (репозиторий Sisyphus), расположенной на территории РФ. Это минимизирует риски атак на цепочки поставок (Supply Chain Attacks).

Для соответствия высоким требованиям ФСТЭК (2-й класс защиты), модель

безопасности «Альт 8 СП» комбинирует политики мандатного управления доступом на базе SELinux с механизмами POSIX Capabilities [8]. Последние позволяют декомпозировать неограниченные права суперпользователя на множество независимых привилегий, снижая поверхность атаки. Контроль запуска исполняемых файлов реализуется за счет строгих мандатных политик SELinux, ограничивающих домены выполнения приложений, в сочетании с проверкой цифровых подписей (GPG) RPM-пакетов на этапе установки и аудита.

4. Сравнительная оценка механизмов защиты

Для систематизации полученных данных авторами разработана сравнительная матрица архитектурных компонентов безопасности (Таблица 1), опирающаяся на базовые требования регулятора.

Таблица 1 — Сравнительная матрица средств защиты отечественных ОС

Критерий оценки	Astra Linux Special Edition	РЕД ОС	ОС «Альт 8 СП»
Теоретическая модель доступа	MAC (Модели Белла-ЛаПадулы и Биба)	MAC (Type Enforcement) + RBAC	MAC (Type Enforcement) + POSIX Capabilities
Реализация в ядре	Собственный модуль Parsec	Стандартный модуль SELinux	Модуль SELinux
Контроль запуска приложений	Встроено в ядро	Утилита fapolicyd (белые	Мандатные политики SELinux +

	(проверка ЭЦП ELF-файлов)	списки, подписи)	проверка подписей RPM (GPG)
Защита адресного пространства	Механизмы ядра (KASLR, PTI, собственные патчи)	ASLR, защита стека (стандартные механизмы)	ASLR, защита стека (стандартные механизмы)
Уничтожение остаточной информации	Встроено в подсистему Parsec (память и диск)	Стандартные средства (shred, srm)	Сертифицированные встроенные утилиты
Сертифицированный класс защиты / Уровень доверия ФСТЭК	Класс 1, УД 1 (Государственная тайна особой важности)	Класс 4, УД 4 (Конфиденциальная информация, КИИ)	Класс 2, УД 2 (Государственная тайна совершенно секретно)

Анализ показывает, что архитектура Parsec в Astra Linux SE, благодаря глубокой интеграции математических моделей изоляции, обеспечивает наиболее проактивный уровень защиты. Это обосновывает ее сертификацию по 1-му классу и делает оптимальным выбором для контуров обработки государственной тайны.
РЕД ОС, применяя механизм Type Enforcement (SELinux), предлагает гранулярную настройку сред выполнения, что является де-факто стандартом для корпоративного сектора, ГИС и медицинских учреждений (УД 4). ОС «Альт 8 СП» (УД 2) компенсирует векторы угроз компрометации базового ПО суверенной инфраструктурой сборки Sisyphus, а использование POSIX

Capabilities эффективно решает проблему единой точки отказа в виде привилегий root.

5. Заключение

Переход на отечественные операционные системы демонстрирует качественный скачок от использования базовых open-source компонентов к созданию глубоко эшелонированных архитектур безопасности. Проведенный структурно-функциональный анализ подтверждает, что выбор конкретной ОС должен базироваться не только на нормативных предписаниях, но и на соответствии встроенных математических моделей безопасности (МАС, ТЕ, МКЦ) актуальной модели нарушителя конкретного предприятия. Учитывая достигнутый предел в интеграции мандатных политик доступа, вектором дальнейших исследований видится разработка авторских методик применения машинного обучения для эвристического анализа логов подсистем аудита (auditd/Parsec), а также перспективы имплементации концепции «Нулевого доверия» (Zero Trust) непосредственно на уровне контроля системных вызовов ядра Linux.

Список литературы

1. Гельфанд А. М. Области применения аналитики больших данных в критических информационных инфраструктурах / А. М. Гельфанд, А. В. Красов, С. И. Штеренберг // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022) : сб. науч. ст. XI Междунар. науч.-техн. и науч.-метод. конф., Санкт-Петербург, 23–24 февраля 2022 г. – СПб. : СПбГУТ, 2022. – С. 438–440.
2. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации : Указ Президента РФ от 01.05.2022 № 250 // Собрание законодательства РФ. – 2022. – № 18. – Ст. 3068.

3. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023) // Собрание законодательства РФ. – 2017. – № 31 (Часть I). – Ст. 4736.
4. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : Приказ ФСТЭК России от 11.02.2013 № 17 // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2013. – № 25.
5. Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1. – М. : ООО «РусБИТех-Астра», 2023. – 340 с.
6. База знаний РЕД ОС [Электронный ресурс] // ООО «РЕД СОФТ» : [сайт]. – URL: https://redos.red-soft.ru/base/ (дата обращения: 25.10.2023).
7. База знаний ОС «Альт» [Электронный ресурс] // ООО «Базальт СПО» : [сайт]. – URL: https://docs.altlinux.org/ru-RU/ (дата обращения: 25.10.2023).
8. Марков, А. С. Опыт сертификации программного обеспечения по требованиям безопасности информации / А. С. Марков, В. Л. Цирлов // Вопросы кибербезопасности. – 2018. – № 1 (25). – С. 45–52.
9. Иванов, А. И. Сравнительный анализ механизмов изоляции процессов в Linux-системах / А. И. Иванов, В. В. Петров // Информационные технологии и безопасность. – 2022. – Т. 14, № 2. – С. 112–118.