УДК 004.056

В.В. БУНИН, А.П. ДУРАКОВСКИЙ

Национальный исследовательский ядерный университет «МИФИ», Москва

РАЗРЕШИТЕЛЬНАЯ СИСТЕМА ДОСТУПА К ФАЙЛОВЫМ СИСТЕМАМ ОС ASTRA LINUX

В работе проведён анализ механизмов разграничения доступа к файловым системам в ОС Astra Linux. Исследована эффективность мандатного контроля доступа (МКД) в сочетании с дискреционной моделью. Рассмотрены проблемы конфигурирования политик Security-Enhanced Linux (SELinux). Разработаны практические рекомендации по повышению защищённости файловых объектов. Предложены новые подходы к автоматизации управления политиками безопасности, расширению аудита и визуализации процессов контроля доступа.

Введение

ОС Astra Linux сертифицирована для применения в государственных и силовых структурах. Её назначение – обеспечение безопасности информации в системах критической информационной инфраструктуры (КИИ) [1]. Это требует использования многоуровневых механизмов регулирования потоков информации, центральное место среди которых занимает разрешительная система доступа к файловым системам. Astra Linux реализует мандатный контроль доступа (МКД) и принудительный контроль на основе политик SELinux [2]. Интеграция дискреционной модели с мандатным контролем на основе меток безопасности позволяет эффективно разграничивать права субъектов [3]. Практическое внедрение этих механизмов сопряжено со сложностями. Настройка МКД и управление политиками SELinux требуют высокой квалификации, ошибки конфигурации могут создавать критические уязвимости [4]. Существующие средства аудита не всегда обеспечивают необходимую детализацию для выявления и расследования инцидентов.

Основные проблемы и предлагаемые решения

Анализ механизмов контроля доступа в Astra Linux выявил комплекс проблем. Основная сложность заключается в конфигурировании политик SELinux, т.к. ручное редактирование конфигурационных файлов требует глубоких специальных знаний и увеличивает вероятность ошибок [4]. Одновременно наблюдается недостаточная гибкость МКД, где жесткая привязка прав к меткам безопасности ограничивает оперативное

перераспределение полномочий [3]. Существенным ограничением являются и возможности системы аудита, фиксирующей лишь базовый набор событий безопасности [2]. Для решения этих проблем предлагается внедрение системы шаблонов политик безопасности для типовых сценариев работы, что упростит развертывание защиты. Одновременно рекомендуется интеграция ролеориентированной модели (RBAC) с существующей системой МКД для реализации механизма временного делегирования полномочий [5]. Совершенствование системы аудита должно включать детальное протоколирование операций с метками безопасности и автоматическое уведомление о подозрительных действиях. Для упрощения работы администраторов предлагается разработка графического интерфейса визуализации политик [4], а для гибридных инфраструктур – модули централизованного управления доступом и инструменты тестирования настроек SELinux [5].

Заключение

Проведённое исследование показало, что Astra Linux обладает развитым аппаратом разграничения доступа на основе интеграции мандатного и дискреционного контроля. Однако механизмы требуют совершенствования в области упрощения управления, повышения гибкости и расширения мониторинга. Предложенные решения – автоматизация управления SELinux, внедрение RBAC, расширение аудита и разработка графических инструментов – направлены на устранение выявленных ограничений. Их реализация позволит снизить нагрузку на администраторов, минимизировать влияние человеческого фактора и повысить устойчивость инфраструктуры к современным угрозам.

Список литературы

1. Иванов Д.В., Гурулев Д.В. Самая безопасная операционная система Astra Linux // Журнал «Трибуна ученого». 2020. Вып. 07. С. 19–27.

2. Девянин П.Н. и др. Интеграция мандатного и ролевого управления доступом в верифицированной модели безопасности ОС // Труды ИСП РАН. 2020. Т. 32. Вып. 1. С. 7–26.

3. Евдокимов О.Г., Гавдан Г.П., Резниченко С.А. Подход к оценке эффективности системы обеспечения ИБ распределённой системы передачи данных // БИТ. 2022. Т. 29. Вып. 2. С. 57–70.

4. Задорожный П.В. Систематизация и анализ средств защиты информации на базе ОС Astra Linux // Наука и просвещение. 2022. С. 54–58.

5. Ильина О.Б., Купчиненко О.П., Скоропад А.В. Изменения в системе защиты информации в ОС Astra Linux SE // ИБРР-2021. С. 152–154.