ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.45

СРАВНЕНИЕ УРОВНЕЙ ЗАЩИЩЕННОСТИ В ОПЕРАЦИОННОЙ СИСТЕМЕ ASTRA LINUX SPECIAL EDITION

Гарманов Сергей Семенович
Кандидат военных наук, полковник запаса, доцент кафедры Общевоенной подготовки,
Военный учебный центр при Российском технологическом университете МИРЭА
119454, г. Москва, Проспект Вернадского, д. 78
Email: garmanov@mirea.ru

Решетников Даниил Дмитриевич
Студент 4 курса
Институт кибербезопасности и цифровых технологий
Российский технологический университет МИРЭА
119454, г. Москва, Проспект Вернадского, д. 78
Email: r.daniil1@outlook.com

Аннотация

Данная статья рассматривает особенности уровней «Орел», «Воронеж», «Смоленск». Перечислены пройденные комплексы испытаний и выполненные требования. Проведено сравнение релизов Common и Special, основных функций систем защиты информации (далее - СЗИ).

Ключевые слова: операционная система Astra Linux Special Edition, информационная безопасность, уровни защищенности.

COMPARSION OF SECURITY LEVELS IN OPERATING SYSTEM ASTRA LINUX SPECIAL EDITION

Sergey S. Garmanov
Candidate of Military Sciences, Reserve Colonel, Associate Professor of the Department of General Military Training
Military Training Center at the Russian Technological University MIREA
78 Prospekt Vernadskogo, Moscow, 119454
Email: garmanov@mirea.ru

Daniil D. Reshetnikov
Student 4 term
Institute of Cybersecurity and Digital Technologies
Russian Technological University MIREA
78 Prospekt Vernadskogo, Moscow, 119454
Email: r.daniil1@outlook.com

ABSTRACT

This article discusses the features of the levels «Orel», «Voronezh», «Smolensk». Listed succeeded complexed test. Comparison of the releases of Common and Special, the main functions of information security systems (hereinafter referred to as ISS).

Keywords: operating system Astra Linux Special Edition, information security, security levels.

В наше время информация является ценным ресурсом в компаниях, поскольку влияет на ее функционирование. Организациям необходимо противостоять большому количеству угроз: промышленный шпионаж, уничтожение данных вирусами и т. д. По этой причине необходимо использовать операционные системы (далее - ОС), которые смогут защитить от различных угроз.

Исходя из этого, мой выбор пал на операционную систему Astra Linux – единственную в стране, которая имеет все сертификаты от Минобороны, Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК) и Федеральной службы безопасности России. Она получила первый уровень доверия за прохождение комплекса испытаний по сертификации СЗИ ФСТЭК. Также соответствует требованиям ОС первого класса защиты и ее безопасности [4].

В настоящее время используется на предприятиях, связанных с оборонной промышленностью, а также используется для обработки информации «особой важности» исходя из сертификата соответствия № 2557 [9]. В нем также указано о наличии в ОС сред виртуализации и систем управления базами данных, что, в свою очередь, подтверждает корректность их применения и реализацию мер защиты.

Существует несколько релизов ОС Astra Linux: Common и Special. Первая подойдет обычным пользователям – с ее помощью можно решать повседневные задачи, не требующие жесткого контроля данных. Образ ОС бесплатный, можно скачать с официального сайта. Версия Special имеет более расширенную и гибкую настройку СЗИ для использования в госструктурах и коммерческих организациях. В ней также можно обрабатывать сведения под грифом «особой важности».

Astra Linux Special Edition имеет три режима защиты: «Базовый», «Усиленный» и «Максимальный» («Орел», «Воронеж» и «Смоленск» соответственно). Последние два включают и дополняют СЗИ, созданные в предыдущих уровнях защиты [1].

Первый режим защиты «Базовый» включает в себя изоляцию процессов, защиту памяти, регистрацию событий безопасности, которые есть в аналогичных дистрибутивах Linux. В нем работает только дискреционное управление доступом. Оно представляет собой взаимодействие нескольких моделей управления доступом: произвольный и на основе списков.

В первой модели у каждого объекта есть один субъект — его владелец, который разрешает или блокирует доступ к нему. Во втором используется таблица, где субъекты и объекты доступа связаны действиями (например удаление), которыми субъект наделен по отношению к объекту. В ней, перед тем как дать или запретить доступ к запрошенным операциям над объектом, система сверяется со списком действий субъекта. В качестве объекта рассматриваются данные, к которым применимы вышеперечисленные действия.

В подсистемах защиты Astra (режим защиты «Орел») и других Linux можно выделить несколько основных недостатков: идентификаторы каждого пользователя и группы являются уникальными только для одного экземпляра ОС; отсутствует изолированная

программная среда, мандатный контроль целостности. Эти, переставшие быть актуальными защитные механизмы, поддерживаются из-за обратной совместимости [3]. Но несмотря на это, такие разработки по-прежнему создают платформу, пригодную для создания ОС. Благодаря им, возможна реализация современных механизмов управления доступом: мандатного и ролевого в последующих режимах защиты. На их основе без значительных изменений можно добиваться теоретического обоснования безопасности и верификации решения. Все это, в результате, позволяет построить защищённую ОС затратив минимальное количество ресурсов.

В режиме «Усиленный» появляются новые СЗИ, такие как: мандатный контроль целостности и замкнутая программная среда. Они используются для повышения защищенности ОС от взлома, заражения различными вирусами, установки закладок, получение привилегий неправомерным доступом и т. д. Эти компоненты входят в подсистему безопасности PARSEC. Она реализует следующие дополнительные функции по работе с устройствами: регистрация устройств в базе учета контроллера или в локальной базе учета; возможность управления доступом к устройствам, используя политику безопасности, основанной на их уровнях конфиденциальности и целостности.

Сравнительно с другими решениями, PARSEC создана с использованием мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками. Она использует три механизма защиты информации: мандатный контроль целостности, мандатное и на основе ролей управление доступом. В сравнении с моделью мандатного управления доступом, реализован мандатный контроль целостности дистрибутива и файловой системы, предусмотрено ролевое управление доступом. Данная модель является единственной в российских ОС, не использующих SELinux (система, реализующая принудительный контроль доступа) как основу.

Эти возможности смогли реализоваться благодаря подсистеме динамического именования устройств udev, которая пришла на замену номерам устройства [2]. «Старший» указывает на соответствие драйвера устройству. Двум разным драйверам может соответствовать одинаковый старший номер. «Младшие» номера позволяют различать отдельные устройства или аппаратные компоненты, управляемые одним драйвером и зависящие от него [6].

Система udev, в свою очередь, позволяет динамически создавать и удалять символические ссылки, а также файлы устройств в каталоге /dev через команду udevadm. С ее помощью возможно изменение порядка её работы, при использовании сценариев bash. В каталоге /dev (благодаря udev) есть только файлы подключенных устройств, соответственно при его отключении они удаляются.

Возможности этой системы udev реализуются системным процессом, работающим в фоновом режиме без непосредственного взаимодействия с пользователем udevd, порядок старта которого указан в сценарии /etc/init.d/udev. Дополнительные для нее параметры описываются в файле /etc/udev/udev.conf.

Во время работы udev может выполнять дополнительные действия, описанные в файлах каталога /etc/udev/rules.d с расширением .rules. Таких операций устройство может иметь больше одного, что позволяет создать для него несколько имен и определить разные действия.

Максимально возможный комплект СЗИ реализован в режиме «Смоленск». В дополнение к дискреционному, здесь используется мандатное управление доступом, назначаемых объектам. Принятие решения о запрете или разрешении доступа субъекта к объекту принимается на основе типа операции мандатного контекста безопасности, связанного с каждым субъектом, и мандатной метки, связанной с объектом. При работе на разных мандатных уровнях и категориях операционная система формально рассматривает

одного и того же пользователя, но с различными мандатными уровнями, как разных пользователей и создаёт для них отдельные домашние каталоги, одновременный прямой доступ пользователя к которым не допускается.

Помимо мандатного управления доступом, этот режим имеет комплекс программ Astra Linux Directory (далее - ALD), который предназначен для организации единого пространства пользователей (далее - ЕПП) в автоматизированных системах. Настройка всех компонентов ALD осуществляется автоматически. Информация о конфигурации сервера и клиентов ALD находятся в файле /etc/ald/ald.conf [7].

В дальнейшем будет использоваться понятие доменная инфраструктура — набор сетевых служб, обеспечивающий централизованное хранение информации об объектах ИТ-инфраструктуры предприятия, предоставляющий механизмы сетевой аутентификации и авторизации.

ЕПП реализует: БД учётных записей пользователей, с возможностью регистрации в доменной сетевой инфраструктуре; удалённые файловые системы и устройства, располагаемые на контроллере домена или файловых серверах, доступ к которым процессы имеют от имени зарегистрированных учётных записей пользователей в соответствии с политикой безопасности.

Здесь, реализацию политики безопасности выполняет модуль, входящий в LSM (Linux security modules) parsec-cifs подсистемы безопасности PARSEC, который активируется на контроллере и клиентах домена в процессе инсталляции с аналогичными ролями. Его функциональные возможности не отличаются от модуля parsec, работающего на компьютерах, которые не входят в состав доменной инфраструктуры. Контроллер домена служит для создания ЕПП, в котором будут авторизоваться пользователи и администраторы [8].

Таким образом, в результате анализа трех уровней защищенности, можно сказать, что наибольшее значение имеют Воронеж и Смоленск, поскольку в них используются свои разработки, являющиеся альтернативой иностранным программным обеспечениям. Например, МРОСЛ ДП-модель, входящая в PARSEC, лишена недостатков, которые присущи мандатному управлению доступом, а также имеет новые возможности [5]. В свою очередь Орел не предоставляет новых возможностей и, более того, дает ограниченный функционал по сравнению с ядром Debian, на котором основана Astra Linux.

Список литературы:

1. Преимущества использования СЗИ в ОС Astra Linux Special Edition – URL: https://habr.com/ru/company/astralinux/blog/670060 (Дата обращения: 04.10.2022)
2. Администрирование устройств - URL: https://yztm.ru/lekc/l8 (Дата обращения: 06.10.2022)
3. Безопасность операционной системы специального назначения Astra Linux Special Edition / под ред. доктора технических наук, профессора П. Н. Девянина. 3-е изд., доп. и перераб. М.: Горячая линия Телеком, 2019. 361 с.
4. Astra Linux Special Edition 1.7 — первый уровень доверия, новое ядро и три уровня защиты – URL: https://astralinux.ru/news/category-news/2021/astra-linux-special-edition-1.7-pervyij-uroven-doveriya-novoe-yadro-i-tri-urovnya-zashhityi (дата обращения 11.10.2022)

5. Русский бронированный Debian. Как устроена новая модель управления доступом в Astra Linux SE – URL: https://xakep.ru/2015/09/15/astra-linux-se (дата обращения 11.10.2022)
6. Номера устройств. Программирование для Linux. Профессиональный подход – URL: https://it.wikireading.ru/34278 (дата обращения 11.10.2022)
7. Astra Linux Directory в Astra Linux Special Edition версии 1.2 – URL: https://wiki.astralinux.ru/pages/viewpage.action?pageId=1212422 (дата обращения 14.10.2022)
8. Использование службы ALD OCCH Astra Linux для защиты информации – URL: https://yztm.ru/lekc/l12 (дата обращения 14.10.2022)
9. Сертификат соответствия №2557 – URL: https://astralinux.ru/information/certificates/sertifikat-sootvetstviya-2557.pdf (дата обращения 14.10.2022)

References:

1. Benefits of using ISS in OS Astra Linux Special Edition
2. Device administration
3. Security of the special-purpose operating system Astra Linux Special Edition / ed. Doctor of Technical Sciences, Professor P. N. Devyanin. 3rd ed., add. and reworked. M.: Hotline Telecom, 2019. 361 p.
4. Astra Linux Special Edition 1.7 - the first level of trust, a new kernel and three levels of protection
5. Russian armored Debian. How the new access control model works in Astra Linux SE
6. Device numbers. Programming for Linux. Professional approach
7. Astra Linux Directory in Astra Linux Special Edition version 1.2
8. Using the ALD OSSN Astra Linux service to protect information
9. Certificate of conformity No. 2557