



ПРИМЕНЕНИЕ СЗИ ОС ASTRA LINUX ДЛЯ ЗАЩИТЫ ОТ УЯЗВИМОСТЕЙ НУЛЕВОГО ДНЯ

Тележников Владимир Юрьевич

Развитие нормативной базы разработки и обеспечения доверия к системному ПО

Разработка и верификация формальных моделей управления доступом

Анализ уязвимостей системного ПО

**НАПРАВЛЕНИЯ
ФОРМИРОВАНИЯ
МЕТОДОЛОГИИ**

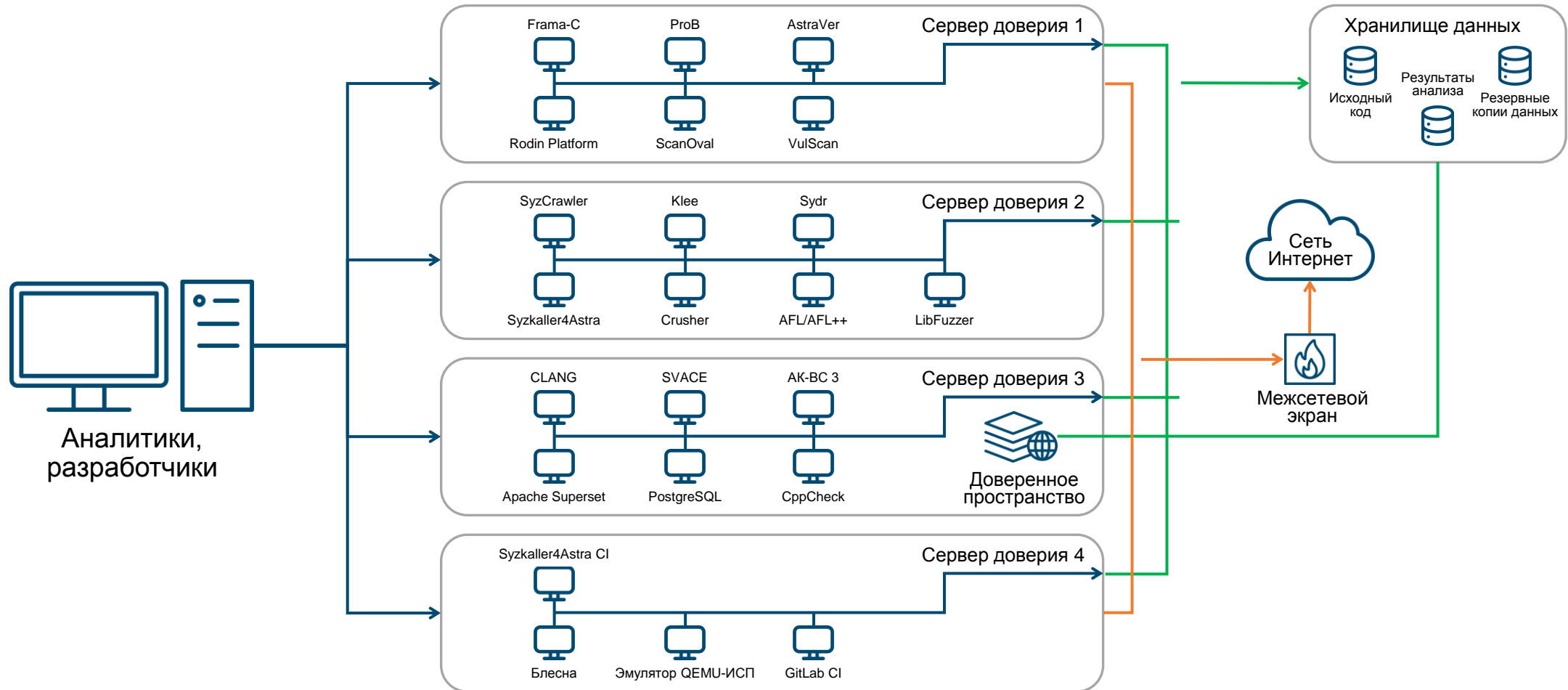
Моделирование угроз разрабатываемого системного ПО

Сбор и аналитическая обработка результатов анализа программного кода системного ПО

Статический и динамический анализ программного кода системного ПО

Архитектурный анализ системного ПО

МАСШТАБИРУЕМАЯ СТРУКТУРА СТЕНДА ДОВЕРИЯ ДЛЯ ВЕРИФИКАЦИИ И АНАЛИЗА КОДА ОПЕРАЦИОННОЙ СИСТЕМЫ



КОМПОНЕНТЫ И РЕЖИМЫ ФУНКЦИОНИРОВАНИЯ СЗИ ОПЕРАЦИОННОЙ СИСТЕМЫ



МРД - МАНДАТНОЕ УПРАВЛЕНИЕ ДОСТУПОМ
(защита информации различных уровней
конфиденциальности)

ПОВЕРХНОСТЬ АТАКИ
(интерфейсы МКЦ, ЗПС, МРД)

**РЕЖИМ
«МАКСИМАЛЬНЫЙ»**
(«Смоленск»)

АДАПТИРОВАННАЯ КОНТЕЙНЕРНАЯ ВИРТУАЛИЗАЦИЯ
(изоляция недоверенных приложений на уровнях МКЦ, «песочницы»,
изоляция приложений на уровнях МРД)

**ЗАПРЕТ УСТАНОВКИ
БИТА ИСПОЛНЕНИЯ**

**БЛОКИРОВКА
ИНТЕРПРЕТАТОРОВ**
(включая bash и
макросы)

**МКЦ. - МАНДАТНЫЙ
КОНТРОЛЬ ЦЕЛОСТНОСТИ**
(защита целостности
программной среды, в т.ч. от
вирусов и закладок)

**ЗПС - ЗАМКНУТАЯ ПРОГРАММНАЯ СРЕДА,
«КИОСК»**
(белый список приложений, их защита от
подмены)

**РЕЖИМ
«УСИЛЕННЫЙ»**
(«Воронеж»)

ДИСКРЕЦИОННОЕ УПРАВЛЕНИЕ ДОСТУПОМ
(защита информации одного уровня конфиденциальности)

**Hardened-
версия ядра ОС**

**РАСШИРЕННЫЙ
АУДИТ СОБЫТИЙ
БЕЗОПАСНОСТИ**

**РЕЖИМ
«БАЗОВЫЙ»**
(«Орел»)

ЯДРО ОС С ИНТЕГРИРОВАННОЙ ПОДДЕРЖКОЙ КОМПЛЕКСА СЗИ

УГРОЗЫ

СБОР ИНФОРМАЦИИ

ПОЛУЧЕНИЕ ПЕРВОНАЧАЛЬНОГО ДОСТУПА

ВНЕДРЕНИЕ И ИСПОЛЬЗОВАНИЕ
ВРЕДНОСНОГО КОДА

ЗАКРЕПЛЕНИЕ В СИСТЕМЕ И СЕТИ

УПРАВЛЕНИЕ ВРЕДНОСНЫМ
КОДОМ И КОМПОНЕНТОМ

ПОВЫШЕНИЕ ПРИВИЛЕГИЙ

СОКРЫТИЕ ДЕЙСТВИЙ

ПОЛУЧЕНИЕ ДОСТУПА
К ДРУГИМ КОМПОНЕНТАМ

СБОР И ВЫВОД ИНФОРМАЦИИ

НЕПРАВОМЕРНЫЙ ДОСТУП ИЛИ ВОЗДЕЙСТВИЕ

МЕРЫ ЗАЩИТЫ

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

ОГРАНИЧЕНИЕ ПРОГРАММНОЙ СРЕДЫ

ОГРАНИЧЕНИЕ ПРОГРАММНОЙ СРЕДЫ

УПРАВЛЕНИЕ ДОСТУПОМ

УПРАВЛЕНИЕ ДОСТУПОМ

РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ,
УПРАВЛЕНИЕ ДОСТУПОМ

УПРАВЛЕНИЕ ДОСТУПОМ,
ЗАЩИТА НОСИТЕЛЕЙ

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ,
УПРАВЛЕНИЕ ДОСТУПОМ

ФУНКЦИИ ЗАЩИТЫ

ФИЛЬТРАЦИЯ ТРАФИКА, И ДР.

ПАРОЛЬНАЯ ПОЛИТИКА, И ДР.

БЛОКИРОВКА ИНТЕРПРЕТАТОРОВ, МАКРОСОВ,
БИТА ИСПОЛНЕНИЯ, МКЦ, ЗПС, КИОСК

КОНТРОЛЬ ЦЕЛОСТНОСТИ, РЕЖИМ «ТОЛЬКО
ЧТЕНИЕ» (OVERLAYFS) И ДР.

ФИЛЬТРАЦИЯ ТРАФИКА, ЗПС,
КОНТРОЛЬ ЦЕЛОСТНОСТИ

МКЦ

МКЦ, КОНТРОЛЬ ЦЕЛОСТНОСТИ

МКЦ, КОНТРОЛЬ ЦЕЛОСТНОСТИ

МКЦ, МРД, УЧЕТ НОСИТЕЛЕЙ

МКЦ, МРД, УЧЕТ НОСИТЕЛЕЙ

НАСЛЕДОВАНИЕ УРОВНЕЙ ЦЕЛОСТНОСТИ ПРИ СОЗДАНИИ ОБЪЕКТОВ



ЗАПУСК СЕРВИСОВ НА ВЫДЕЛЕННОМ УРОВНЕ ЦЕЛОСТНОСТИ

Управление политикой безопасности - Режим эксперта

Настройки мандатного контроля целостности

Управление Режим эксперта

Максимальный уровень целостности (текущий): 63 - Высокий

Максимальный уровень целостности (в загрузчике): 63 - Высокий

Целостность файловой системы (fs-ilev.conf) Сервисы

Включено

Отметить все элементы по умолчанию

Файловая система Редактирование конфига Исключения

Имя	Текущий уровень целостности	У
/	63 - Высокий	—
bin	63 - Высокий	М
boot	63 - Высокий	М
dev	63 - Высокий	—
etc	63 - Высокий	М
home	63 - Высокий	—
astra	63 - Высокий	—
test	0 - Низкий	—
lib	63 - Высокий	М
apt	63 - Высокий	—
aspell	63 - Высокий	—
astra-safepolicy	63 - Высокий	—
at-spi2-core	63 - Высокий	—

Подсказка: используйте двойной щелчок на уровне чтобы его изменить

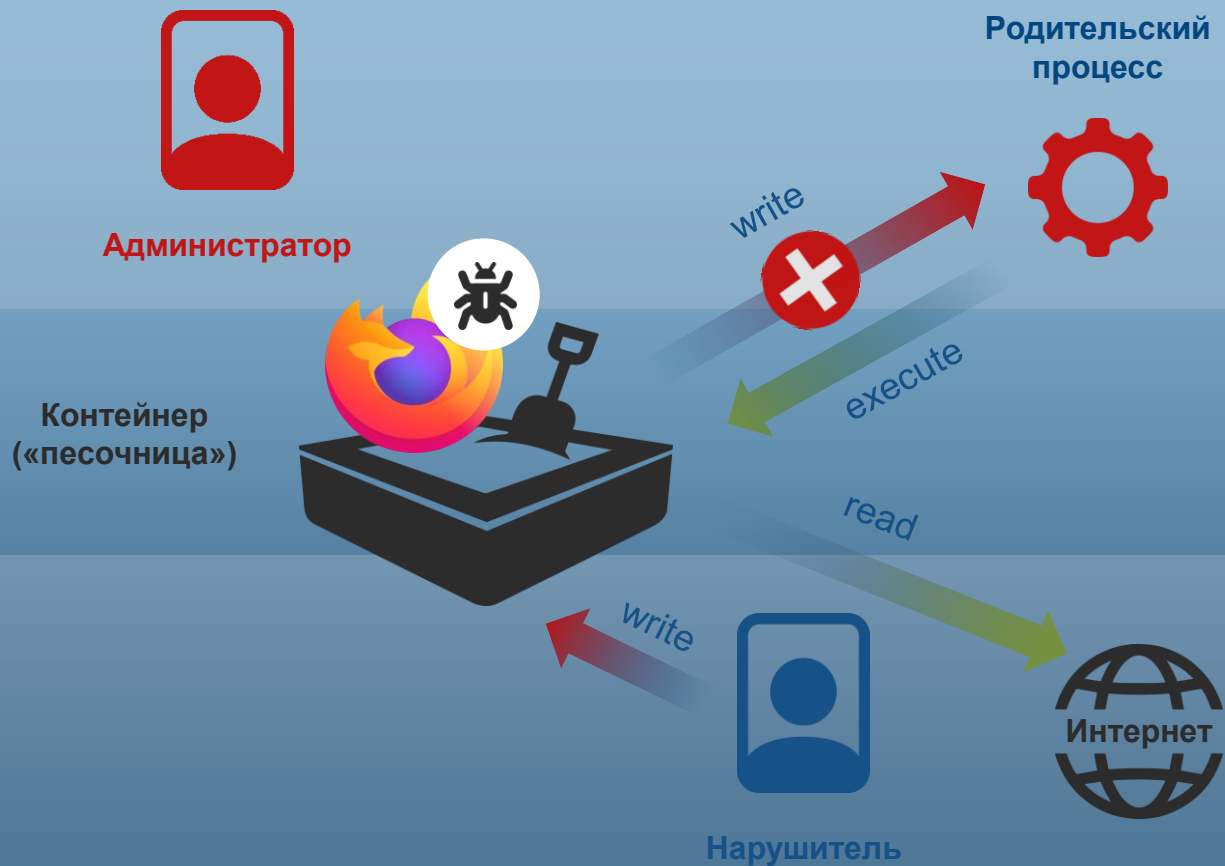
ASTRA LINUX®

13:40
ВТ, 21 ИЮН

ПРИМЕР ИСПОЛЬЗОВАНИЯ МКЦ ДЛЯ БЕЗОПАСНОГО ЗАПУСКА ПРИЛОЖЕНИЙ



ПРИМЕР ИСПОЛЬЗОВАНИЯ МКЦ ДЛЯ БЕЗОПАСНОГО ЗАПУСКА ПРИЛОЖЕНИЙ



↑
63 Высокий уровень целостности

↓
2 Промежуточный уровень целостности

ЗАПУСК СЕРВИСОВ НА ВЫДЕЛЕННОМ УРОВНЕ ЦЕЛОСТНОСТИ



«НИЗКИЙ» УРОВЕНЬ

СЕТЕВЫЕ СЕРВИСЫ

ВИРТУАЛИЗАЦИЯ

КОНТЕЙНЕРИЗАЦИЯ

ГРАФИЧЕСКИЙ СЕРВЕР

СУБД

АНТИВИРУСНЫЕ СРЕДСТВА

«ВЫСОКИЙ» УРОВЕНЬ

КОНТРОЛЛЕР ДОМЕНА

ГИПЕРВИЗОР

Управление политикой безопасности - Монитор безопасности

Подсистема	Статус
8 Мандатный Контроль Целостности на файловой системе	✓
9 Запрет установки бита исполнения	✓
10 Блокировка трассировки ptrace	✓
11 Блокировка одновременной работы с разными уровнями sumac	✓
12 Блокировка клавиш SysRq	✓
13 Межсетевой экран UFW	✗
14 Системные ограничения ulimits	✗
15 Блокировка выключения/перезагрузки ПК для пользователей	✓
16 Запрет монтирования носителей непривилегированным пользователям	✓
17 Режим ЗПС (замкнутой программной среды) в исполняемых файлах	✓
18 Режим ЗПС (замкнутой программной среды) в расширенных атрибутах	✓
19 Безопасное удаление	✗
20 Режим работы файловой системы ОС - только чтение	✗
21 Ввод пароля для sudo	✓
22 Системный кiosk	✓
23 Графический кiosk	✗
24 Сервисы на уровне МКЦ 1	✓
25 Docker на уровне МКЦ 2	✓

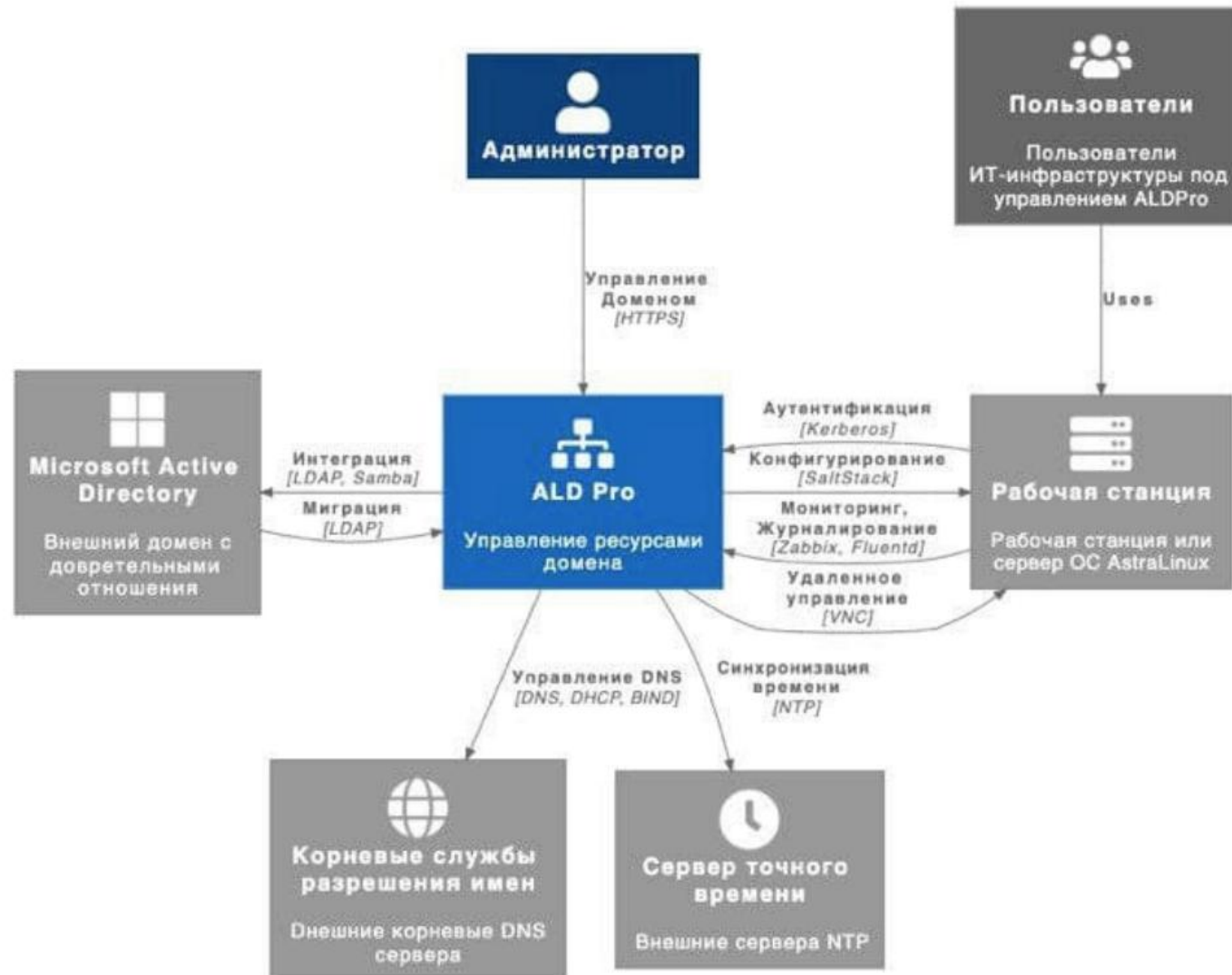
Настроить Мандатный Контроль Целостности на файловой системе



ALD PRO ЦЕНТРАЛИЗОВАННАЯ НАСТРОЙКА СЗИ



- УПРАВЛЕНИЕ ДОМЕНОМ
- ГРУППОВЫЕ ПОЛИТИКИ
- НАСТРОЙКА КОНФИГУРАЦИЙ
- ...
- УСТАНОВКА И ОБНОВЛЕНИЕ ПО
- НАСТРОЙКА И КОНТРОЛЬ СЗИ**
- АУДИТ СОБЫТИЙ БЕЗОПАСНОСТИ
- МОНИТОРИНГ БЕЗОПАСНОСТИ



ВОЗМОЖНОСТИ СЗИ ОПЕРАЦИОННОЙ СИСТЕМЫ ПО НЕЙТРАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ



Пересчет уровней критичности уязвимостей при активации СЗИ ОС Astra Linux на примере уязвимости в Polkit (CVE-2021-4034)

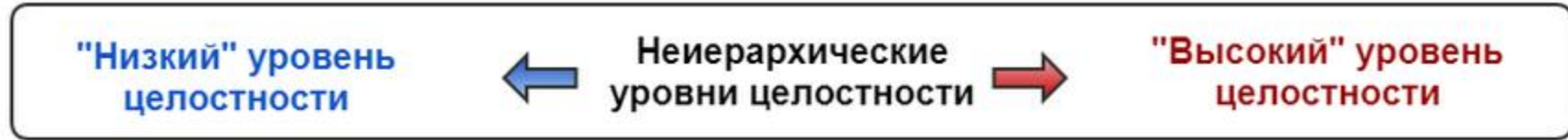
Базовые метрики CVSS	ОС Astra Linux в базовом режиме функционирования	ОС Astra Linux с включенным МКЦ	ОС Astra Linux с включенными МКЦ и ЗПС*	ОС Astra Linux с включенными МКЦ, ЗПС и блокировкой интерпретаторов*	ОС Astra Linux с дополнительно включенным МРД
Вектор атаки (AV):	Локальный (L)	Локальный (L)	Локальный (L)	Локальный (L)	Локальный (L)
Сложность атаки (AC):	Низкая (L)	Низкая (L)	Высокая (H)	Высокая (H)	Высокая (H)
Уровень привилегий (PR):	Низкий (L)	Низкий (L)	Высокий (H)	Высокий (H)	Высокий (H)
Взаимодействие с пользователем (UI):	Не требуется (N)	Не требуется (N)	Не требуется (N)	Требуется (R)	Требуется (R)
Влияние на другие компоненты системы (S):	Не оказывает (U)	Не оказывает (U)	Не оказывает (U)	Не оказывает (U)	Не оказывает (U)
Влияние на конфиденциальность (C):	Высокое (H)	Высокое (H)	Высокое (H)	Высокое (H)	Не оказывает (N)
Влияние на целостность (I):	Высокое (H)	Низкое (L)	Низкое (L)	Низкое (L)	Низкое (L)
Влияние на доступность (A):	Высокое (H)	Низкое (L)	Низкое (L)	Низкое (L)	Низкое (L)
Итоговый уровень критичности:	7.8 (Высокий)	6.6 (Средний)	5.2 (Средний)	5.1 (Средний)	2.9 (Низкий)

* - в случае, если нарушителю вообще удастся проэксплуатировать уязвимость!

ПРИМЕР ИСПОЛЬЗОВАНИЯ МКЦ ДЛЯ КОНТЕЙНЕРНОЙ ВИРТУАЛИЗАЦИИ



ПРИМЕР ИСПОЛЬЗОВАНИЯ МКЦ ДЛЯ КОНТЕЙНЕРНОЙ ВИРТУАЛИЗАЦИИ



PostgreSQL

LibreOffice

exim

APACHE
HTTP SERVER PROJECT

python™

BASH
THE BOURNE-AGAIN SHELL



КОМПОНЕНТЫ И РЕЖИМЫ ФУНКЦИОНИРОВАНИЯ СЗИ ОПЕРАЦИОННОЙ СИСТЕМЫ



МРД - МАНДАТНОЕ УПРАВЛЕНИЕ ДОСТУПОМ
(защита информации различных уровней
конфиденциальности)

ПОВЕРХНОСТЬ АТАКИ
(интерфейсы МКЦ, ЗПС, МРД)

**РЕЖИМ
«МАКСИМАЛЬНЫЙ»**
(«Смоленск»)

АДАПТИРОВАННАЯ КОНТЕЙНЕРНАЯ ВИРТУАЛИЗАЦИЯ
(изоляция недоверенных приложений на уровнях МКЦ, «песочницы»,
изоляция приложений на уровнях МРД)

**ЗАПРЕТ УСТАНОВКИ
БИТА ИСПОЛНЕНИЯ**

**БЛОКИРОВКА
ИНТЕРПРЕТАТОРОВ**
(включая bash и
макросы)

**МКЦ. - МАНДАТНЫЙ
КОНТРОЛЬ ЦЕЛОСТНОСТИ**
(защита целостности
программной среды, в т.ч. от
вирусов и закладок)

**ЗПС - ЗАМКНУТАЯ ПРОГРАММНАЯ СРЕДА,
«КИОСК»**
(белый список приложений, их защита от
подмены)

**РЕЖИМ
«УСИЛЕННЫЙ»**
(«Воронеж»)

ДИСКРЕЦИОННОЕ УПРАВЛЕНИЕ ДОСТУПОМ
(защита информации одного уровня конфиденциальности)

**Hardened-
версия ядра ОС**

**РАСШИРЕННЫЙ
АУДИТ СОБЫТИЙ
БЕЗОПАСНОСТИ**

**РЕЖИМ
«БАЗОВЫЙ»**
(«Орел»)

ЯДРО ОС С ИНТЕГРИРОВАННОЙ ПОДДЕРЖКОЙ КОМПЛЕКСА СЗИ



Спасибо за внимание!