ПРИМЕНЕНИЕ СЗИ ОС ASTRA LINUX ДЛЯ ЗАЩИТЫ ОТ УЯЗВИМОСТЕЙ НУЛЕВОГО ДНЯ

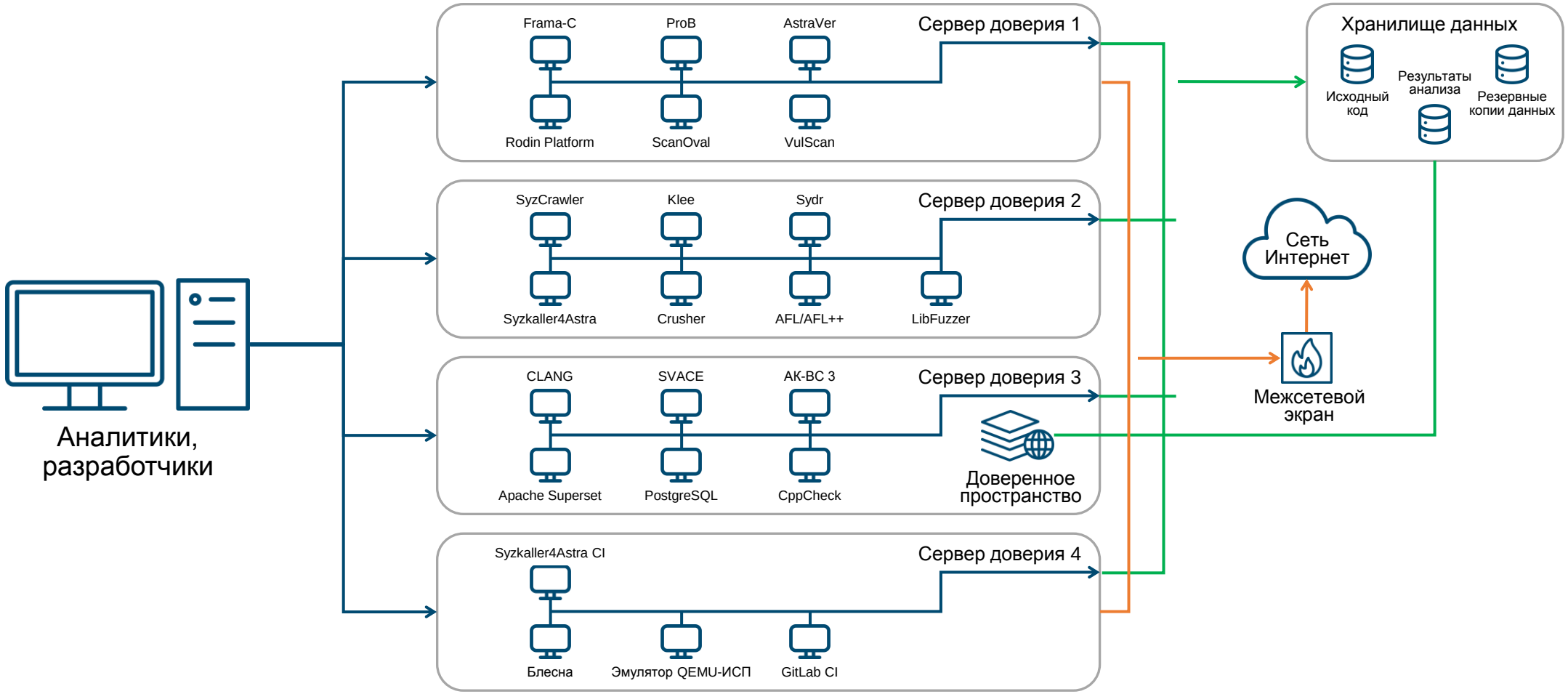
Тележников Владимир Юрьевич

РАЗРАБОТКА БЕЗОПАСНОГО СИСТЕМНОГО ПО

ASTRA LINUX®

- Развитие нормативной базы разработки и обеспечения доверия к системному ПО
- Разработка и верификация формальных моделей управления доступом
- Анализ уязвимостей системного ПО
- 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

ASTRA LINUX®

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

ПОВЕРХНОСТЬ АТАКИ
(интерфейсы МКЦ, ЗПС, МРД)

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 «МАКСИМАЛЬНЫЙ» («Смоленск»)

РЕЖИМ «УСИЛЕННЫЙ» («Воронеж»)

ДИСКРЕЦИОННОЕ УПРАВЛЕНИЕ ДОСТУПОМ
(защита информации одного уровня конфиденциальности)

Hardened-версия ядра ОС

РАСШИРЕННЫЙ АУДИТ СОБЫТИЙ БЕЗОПАСНОСТИ

ЯДРО ОС С ИНТЕГРИРОВАННОЙ ПОДДЕРЖКОЙ КОМПЛЕКСА СЗИ

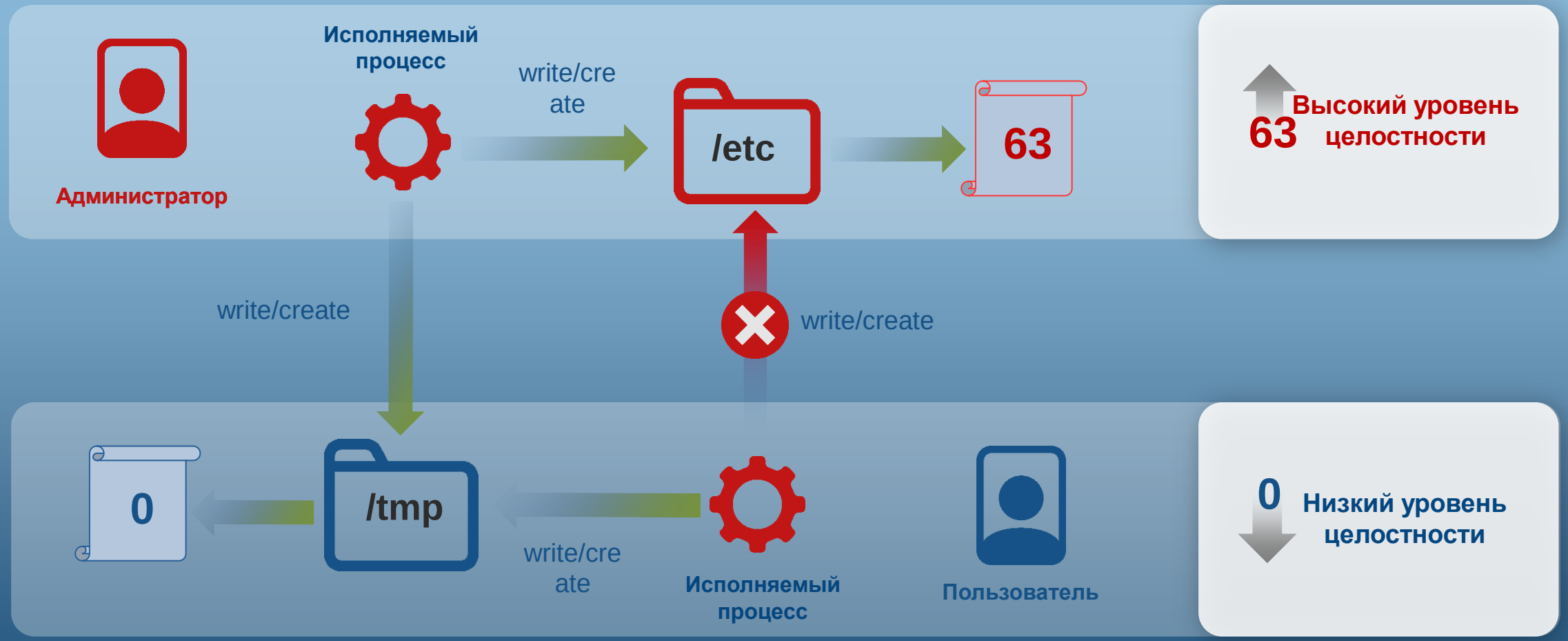
РЕЖИМ «БАЗОВЫЙ» («Орел»)

ЗАЩИТА ОТ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

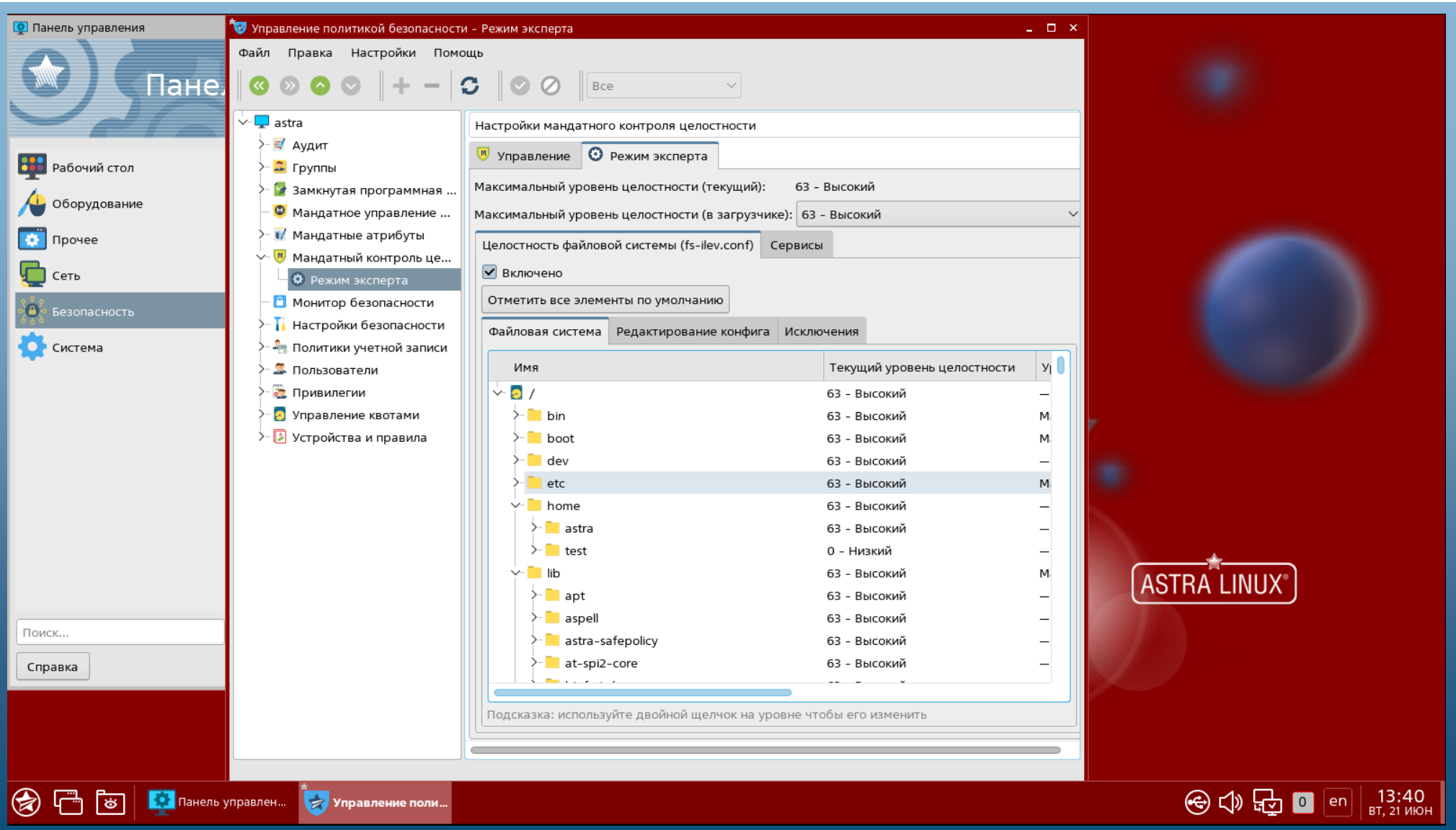
ASTRA LINUX®

УГРОЗЫ	МЕРЫ ЗАЩИТЫ	ФУНКЦИИ ЗАЩИТЫ
СБОР ИНФОРМАЦИИ	ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ	ФИЛЬТРАЦИЯ ТРАФИКА, И ДР.
ПОЛУЧЕНИЕ ПЕРВОНАЧАЛЬНОГО ДОСТУПА	ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ	ПАРОЛЬНАЯ ПОЛИТИКА, И ДР.
ВНЕДРЕНИЕ И ИСПОЛЬЗОВАНИЕ ВРЕДОНОСНОГО КОДА	ОГРАНИЧЕНИЕ ПРОГРАММНОЙ СРЕДЫ	БЛОКИРОВКА ИНТЕРПРЕТАТОРОВ, МАКРОСОВ, БИТА ИСПОЛНЕНИЯ, МКЦ, ЗПС, КИОСК
ЗАКРЕПЛЕНИЕ В СИСТЕМЕ И СЕТИ	ОГРАНИЧЕНИЕ ПРОГРАММНОЙ СРЕДЫ	КОНТРОЛЬ ЦЕЛОСТНОСТИ, РЕЖИМ «ТОЛЬКО ЧТЕНИЕ» (OVERLAYFS) И ДР.
УПРАВЛЕНИЕ ВРЕДОНОСНЫМ КОДОМ И КОМПОНЕНТОМ	УПРАВЛЕНИЕ ДОСТУПОМ	ФИЛЬТРАЦИЯ ТРАФИКА, ЗПС, КОНТРОЛЬ ЦЕЛОСТНОСТИ
ПОВЫШЕНИЕ ПРИВИЛЕГИЙ	УПРАВЛЕНИЕ ДОСТУПОМ	МКЦ
СОКРЫТИЕ ДЕЙСТВИЙ	РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ	МКЦ, КОНТРОЛЬ ЦЕЛОСТНОСТИ
ПОЛУЧЕНИЕ ДОСТУПА К ДРУГИМ КОМПОНЕНТАМ	ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ, УПРАВЛЕНИЕ ДОСТУПОМ	МКЦ, КОНТРОЛЬ ЦЕЛОСТНОСТИ
СБОР И ВЫВОД ИНФОРМАЦИИ	УПРАВЛЕНИЕ ДОСТУПОМ, ЗАЩИТА НОСИТЕЛЕЙ	МКЦ, МРД, УЧЕТ НОСИТЕЛЕЙ
НЕПРАВОМЕРНЫЙ ДОСТУП ИЛИ ВОЗДЕЙСТВИЕ	ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ, УПРАВЛЕНИЕ ДОСТУПОМ	МКЦ, МРД, УЧЕТ НОСИТЕЛЕЙ

НАСЛЕДОВАНИЕ УРОВНЕЙ ЦЕЛОСТНОСТИ ПРИ СОЗДАНИИ ОБЪЕКТОВ



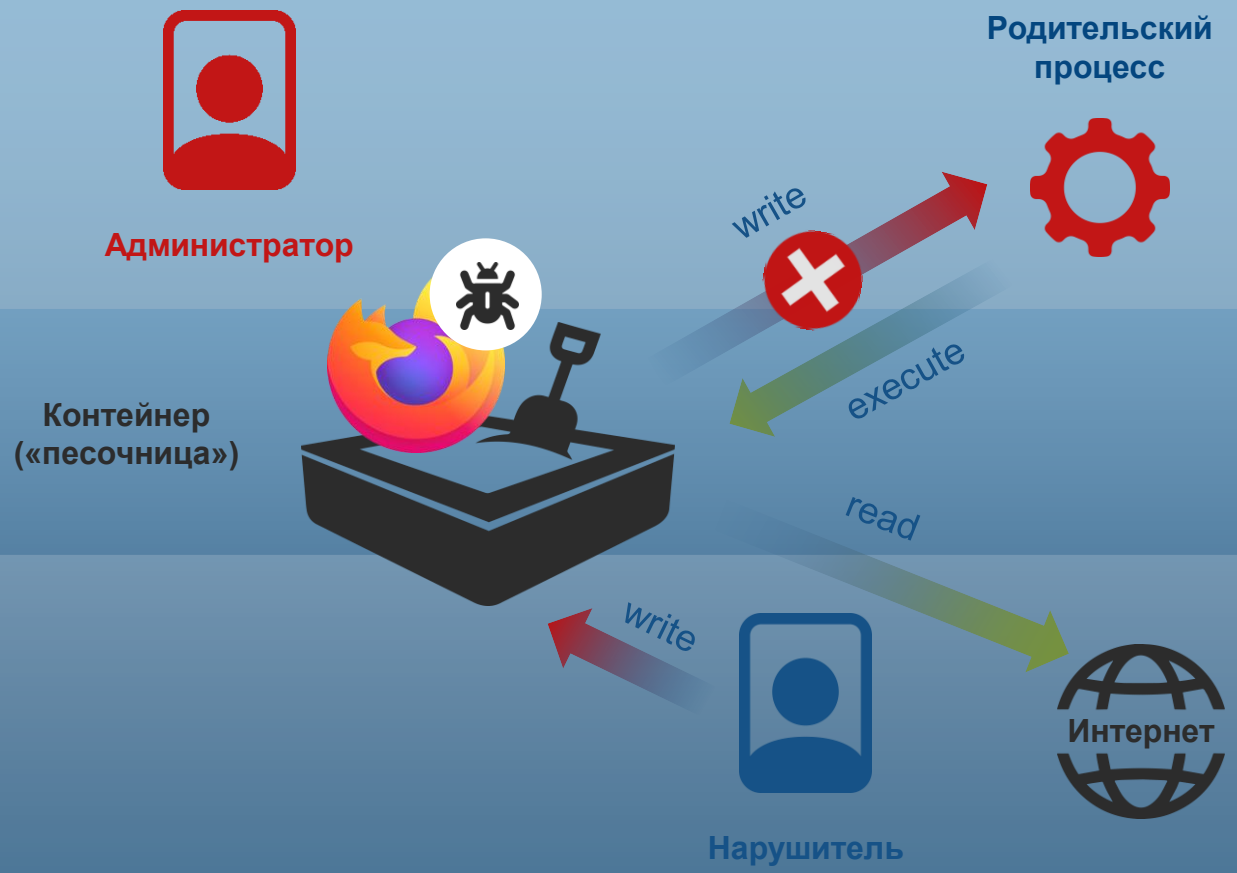
ЗАПУСК СЕРВИСОВ НА ВЫДЕЛЕННОМ УРОВНЕ ЦЕЛОСТНОСТИ



ПРИМЕР ИСПОЛЬЗОВАНИЯ МКЦ ДЛЯ БЕЗОПАСНОГО ЗАПУСКА ПРИЛОЖЕНИЙ

ПРИМЕР ИСПОЛЬЗОВАНИЯ МКЦ ДЛЯ БЕЗОПАСНОГО ЗАПУСКА ПРИЛОЖЕНИЙ

ASTRA LINUX®



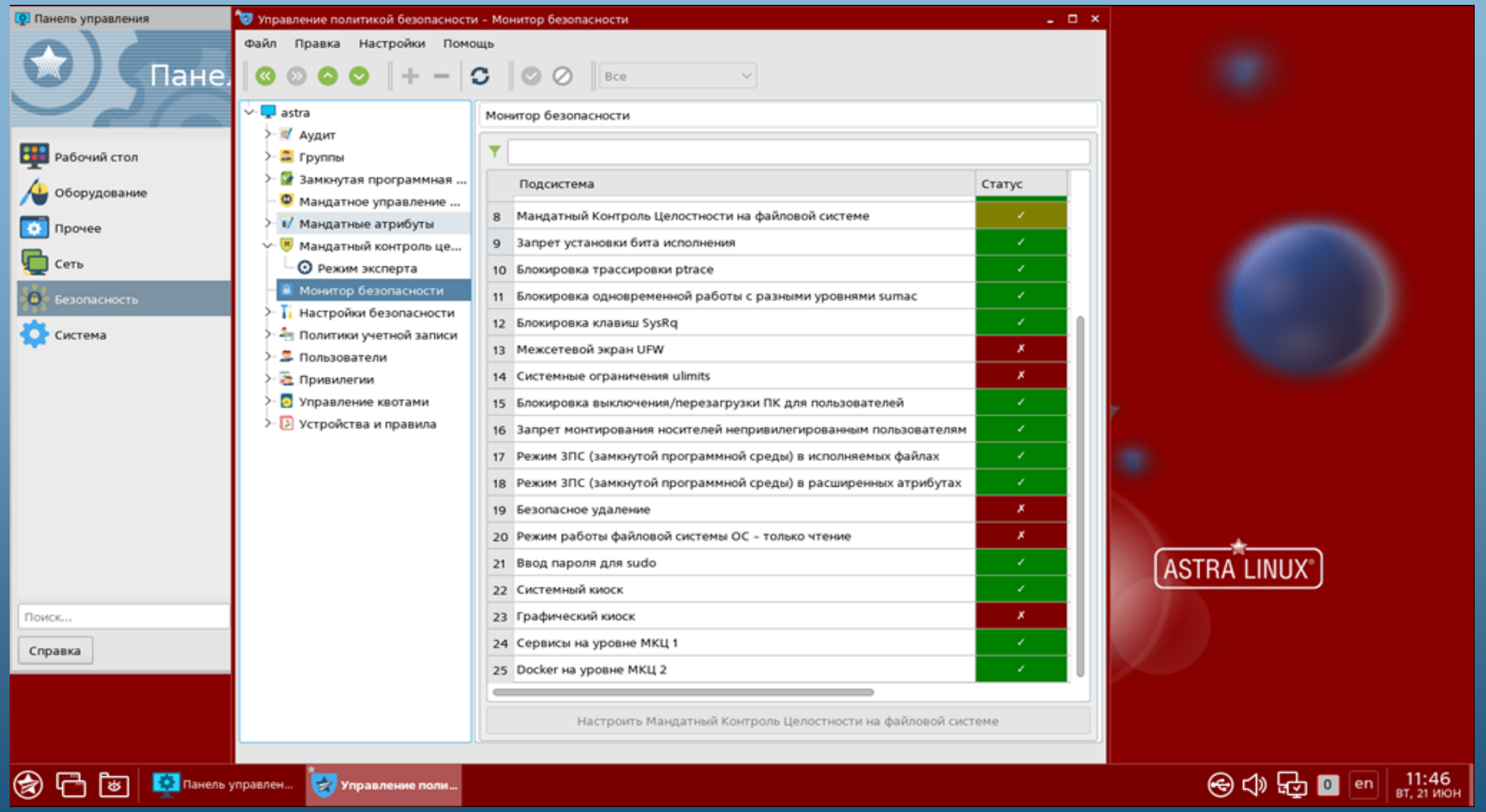
63 Высокий уровень целостности

2 Промежуточный уровень целостности

ЗАПУСК СЕРВИСОВ НА ВЫДЕЛЕННОМ УРОВНЕ ЦЕЛОСТНОСТИ

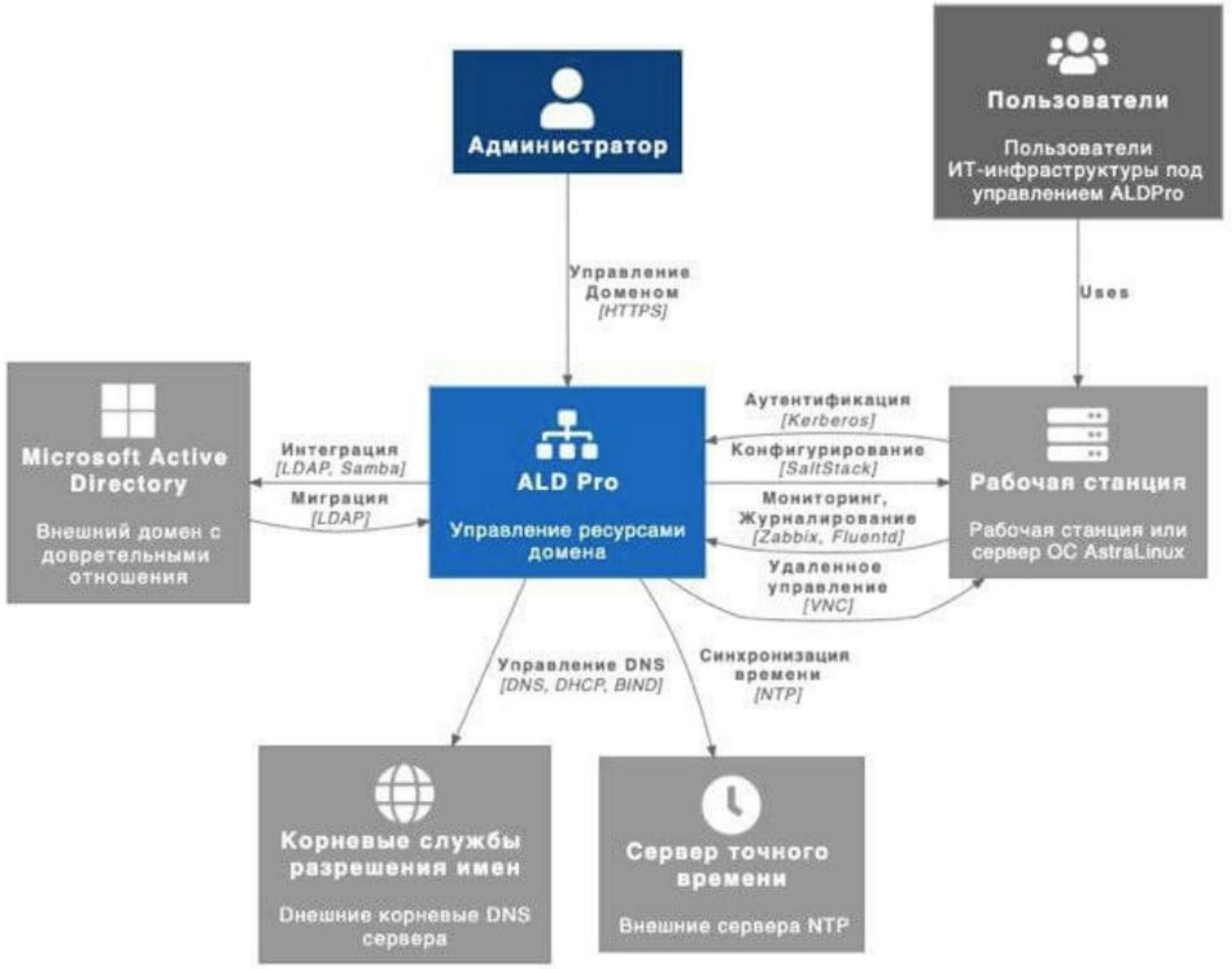
ASTRA LINUX®

- «НИЗКИЙ» УРОВЕНЬ
- СЕТЕВЫЕ СЕРВИСЫ
- ВИРТУАЛИЗАЦИЯ
- КОНТЕЙНЕРИЗАЦИЯ
- ГРАФИЧЕСКИЙ СЕРВЕР
- СУБД
- АНТИВИРУСНЫЕ СРЕДСТВА
- «ВЫСОКИЙ» УРОВЕНЬ
- КОНТРОЛЛЕР ДОМЕНА
- ГИПЕРВИЗОР



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

ASTRA LINUX®

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

ASTRA LINUX®

"Низкий" уровень целостности ← Неиерархические уровни целостности → "Высокий" уровень целостности

docker

PostgreSQL

LibreOffice

exim

APACHE HTTP SERVER PROJECT

python™

BASH THE BOURNE-AGAIN SHELL

Линейные уровни целостности

127

-128

КОМПОНЕНТЫ И РЕЖИМЫ ФУНКЦИОНИРОВАНИЯ СЗИ ОПЕРАЦИОННОЙ СИСТЕМЫ

ASTRA LINUX®

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

ПОВЕРХНОСТЬ АТАКИ
(интерфейсы МКЦ, ЗПС, МРД)

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 «МАКСИМАЛЬНЫЙ» («Смоленск»)

РЕЖИМ «УСИЛЕННЫЙ» («Воронеж»)

ДИСКРЕЦИОННОЕ УПРАВЛЕНИЕ ДОСТУПОМ
(защита информации одного уровня конфиденциальности)

Hardened-версия ядра ОС

РАСШИРЕННЫЙ АУДИТ СОБЫТИЙ БЕЗОПАСНОСТИ

ЯДРО ОС С ИНТЕГРИРОВАННОЙ ПОДДЕРЖКОЙ КОМПЛЕКСА СЗИ

РЕЖИМ «БАЗОВЫЙ» («Орел»)

ASTRA LINUX®

Спасибо за внимание!