



Использование мандатного контроля целостности для изолированного запуска средств контейнеризации в ОС Astra Linux

Руководитель направления
Старостин А.А.





>>>> Мандатный контроль целостности

2018 (Астра 1.6)

2018 (1.6)

0..255

Неиерархический уровень

↑ **63 (0b00111111) - «Высокий»**

↑ **0 (0b00000000) - «Низкий»**





>>>> Мандатный контроль целостности

2021 (Астра 1.7)

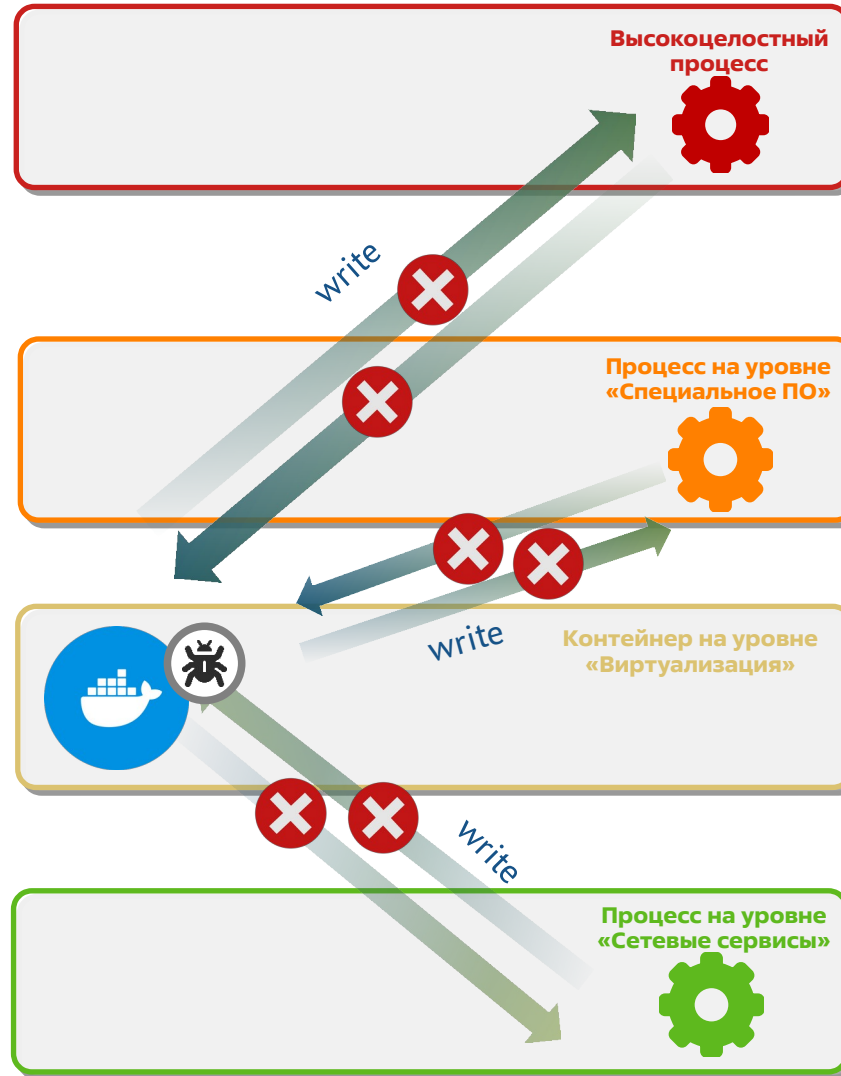
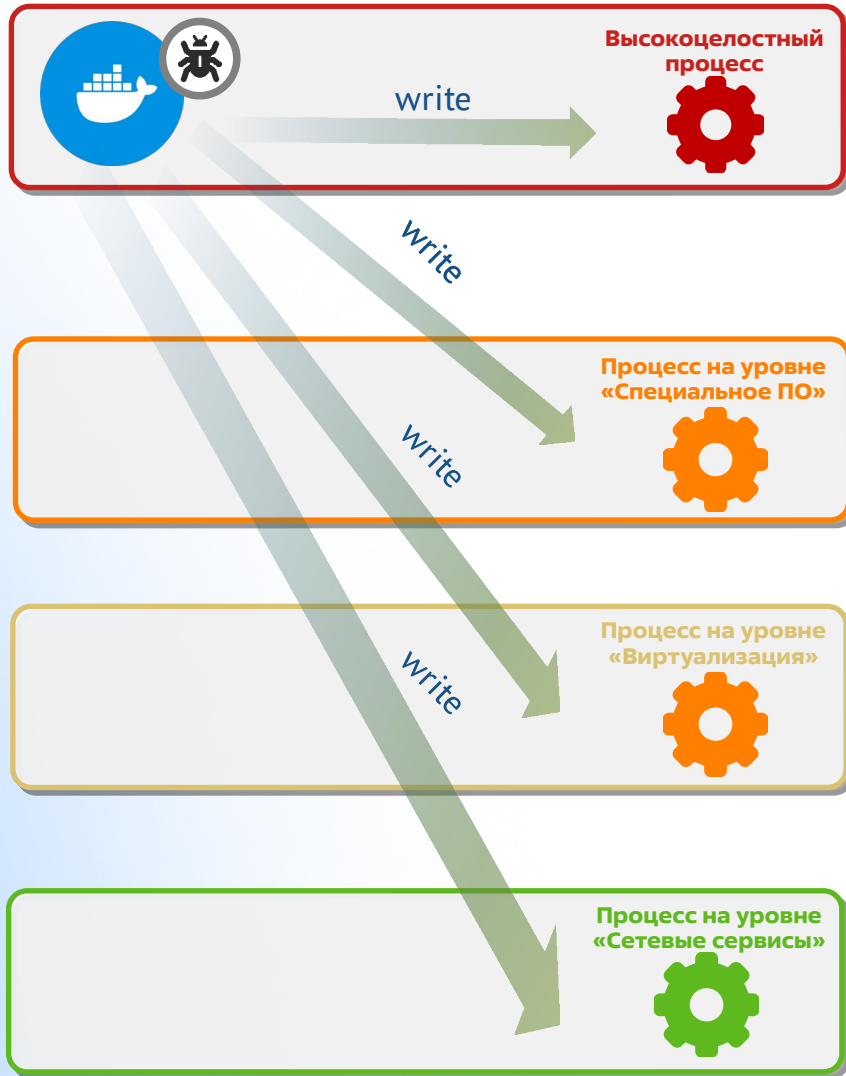


- ↑ **63** (0b00111111) - «Высокий»
- ↑ **32** (0b00100000) - «Виртуальные машины»
- ↑ **16** (0b00010000) - «СУБД»
- ↑ **8** (0b00001000) - «Графический сервер»
- ↑ **4** (0b00000100) - «Специальное ПО»
- ↑ **2** (0b00000010) - «Виртуализация»
- ↑ **1** (0b00000001) - «Сетевые сервисы»
- ↑ **0** (0b00000000) - «Низкий»



Использование промежуточных уровней

Запуск ПО в сессии высокоцелостного администратора



63

Высокий уровень целостности

4

Промежуточный уровень целостности «Специальное ПО»

2

Промежуточный уровень целостности «Виртуализация»

1

Промежуточный уровень целостности «Сетевые сервисы»



Адаптированная контейнерная виртуализация

Типы атак на контейнеры

ПОБЕГ ИЗ КОНТЕЙНЕРА

Уязвимости в ПО контейнера для получения доступа к хосту

МЕЖКОНТЕЙНЕРНЫЕ АТАКИ

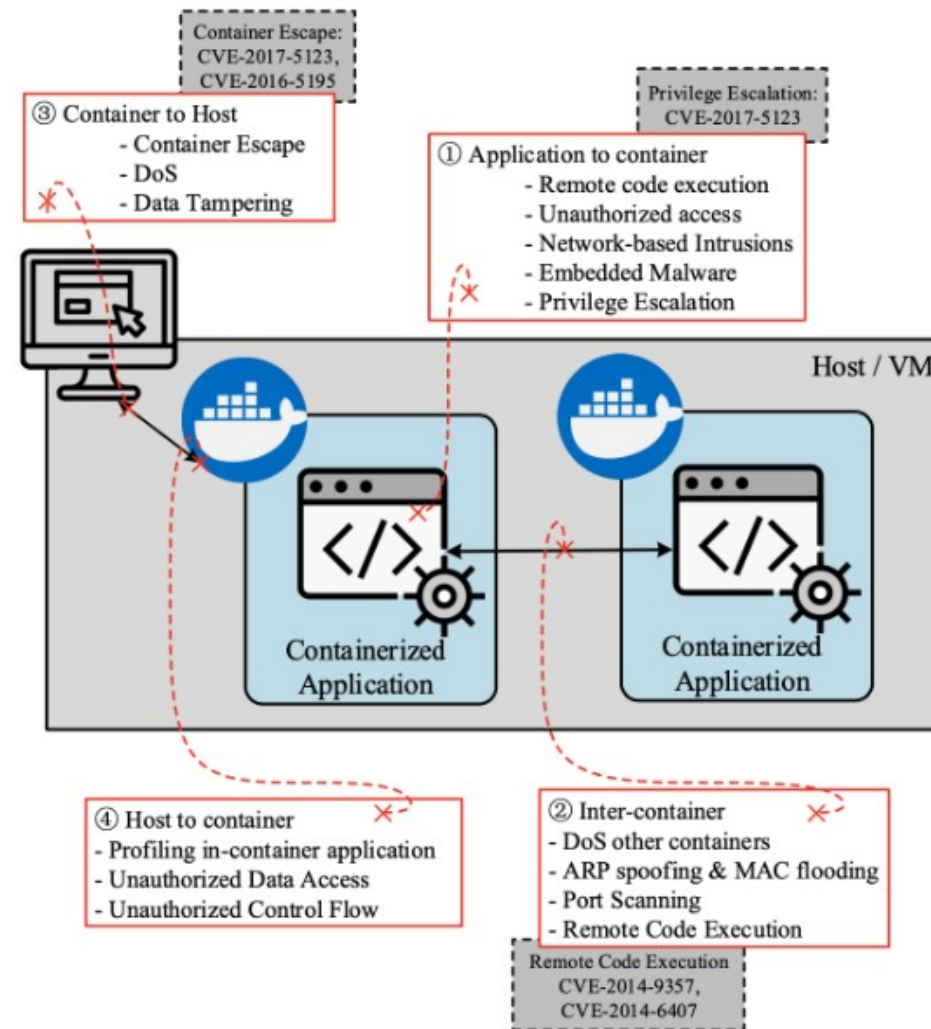
Компрометация соседних контейнеров

АТАКИ НА КОНТЕЙНЕР

защита информации в безопасных контейнерах

ВНЕШНИЕ АТАКИ НА КОНТЕЙНЕР

защита информации в контейнерах





>>>> Линейные уровни целостности

Особенности

ИЕРАРХИЧНОСТЬ

Возможность сравнения различных уровней между собой

ШИРОКИЙ ДИАПАЗОН ЗНАЧЕНИЙ

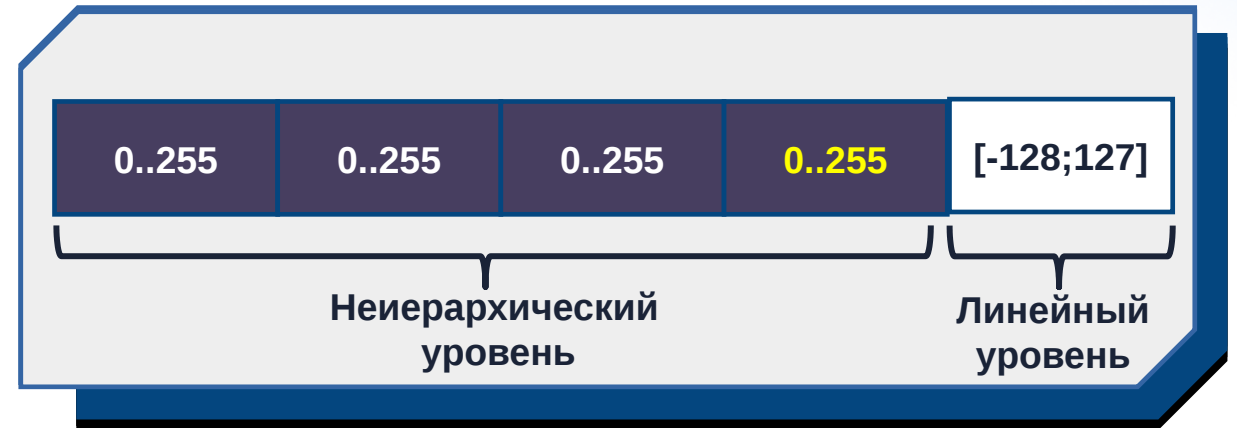
От -128 до +127

ПОЛОЖИТЕЛЬНЫЙ УРОВЕНЬ ЦЕЛОСТНОСТИ

Возможность защиты «доверенных» приложений

ОТРИЦАТЕЛЬНЫЙ УРОВЕНЬ ЦЕЛОСТНОСТИ

Реализация полноценной «песочницы»





>>>> Линейные уровни целостности

Правила доступа



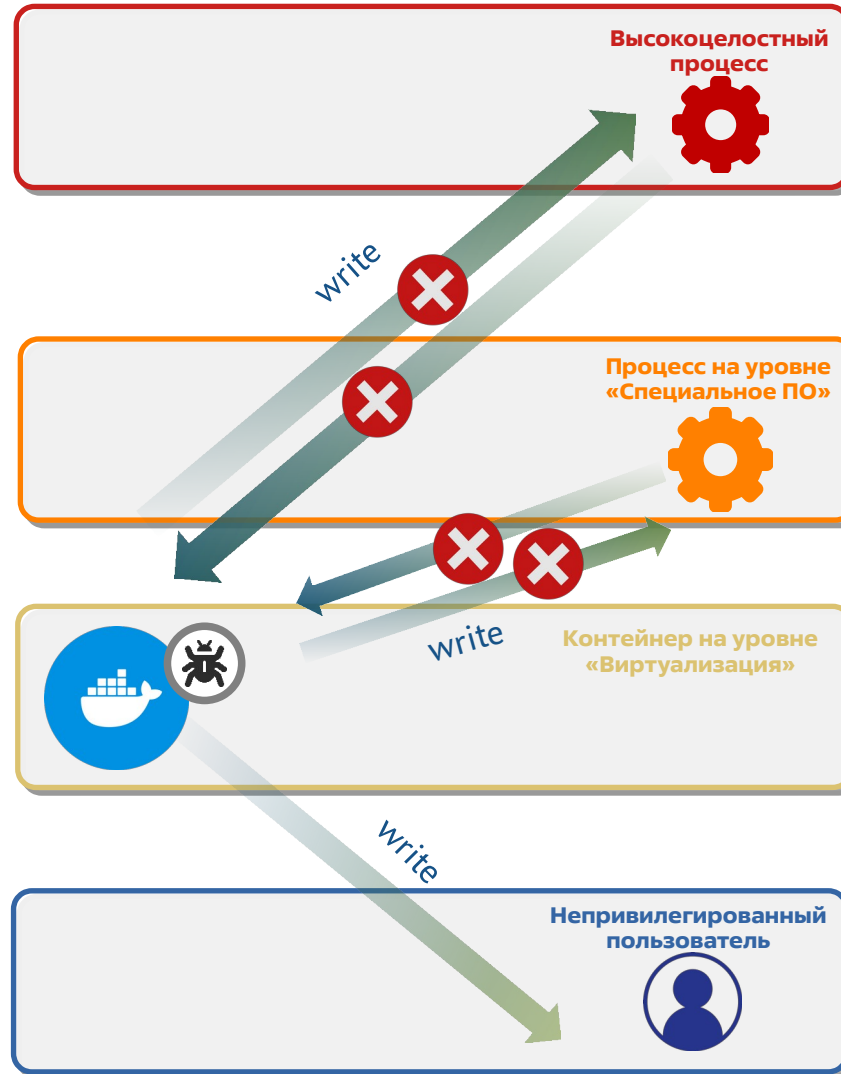
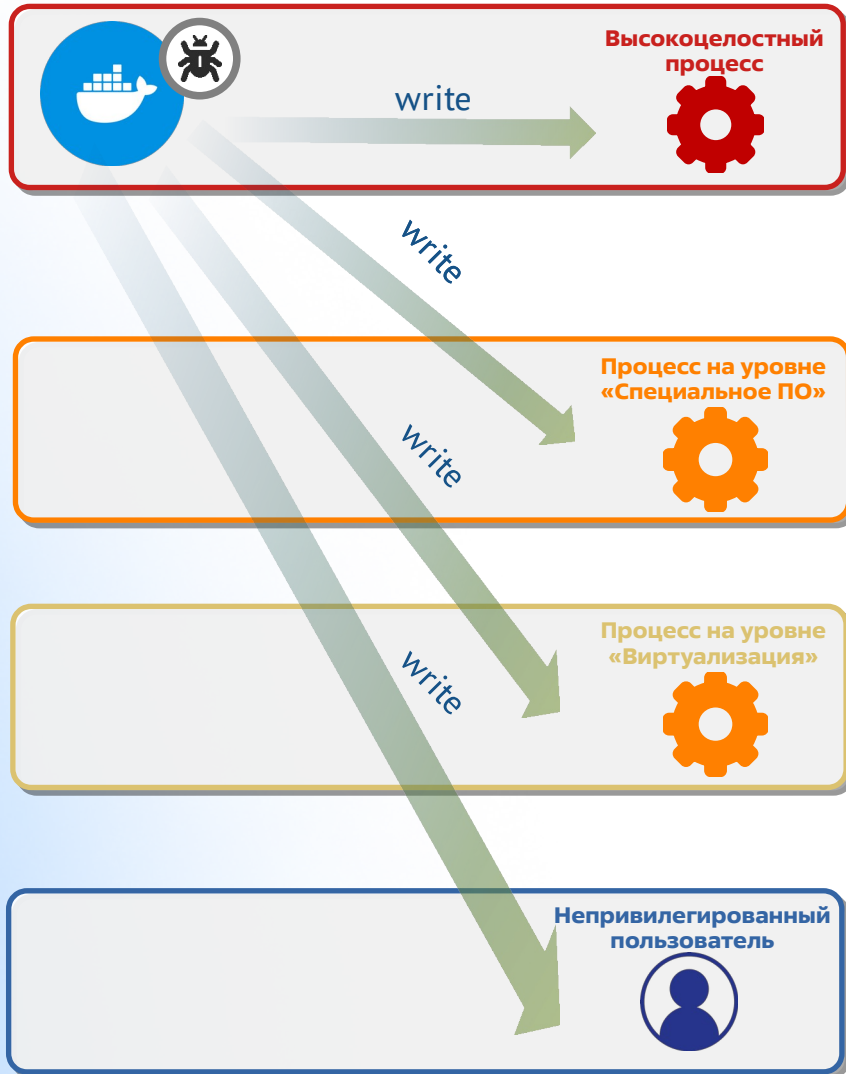
2

Промежуточный
уровень
целостности
«Виртуализация»



Использование промежуточных уровней

Запуск ПО в сессии высокоцелостного администратора



- 63**
Высокий уровень целостности
- 4**
Промежуточный уровень целостности «Специальное ПО»
- 2**
Промежуточный уровень целостности «Виртуализация»
- 0**
Низкий уровень целостности



>>>> Адаптированная контейнерная виртуализация

Защита непривилегированного пользователя



0
Низкий
уровень
целостности



0
Низкий
уровень
целостности



Адаптированная контейнерная виртуализация

Защита от «межконтейнерных» атак



2
Промежуточный
уровень
целостности
«Виртуализация»



2
Промежуточный
уровень
целостности
«Виртуализация»



>>>> Адаптированная контейнерная виртуализация

Защита контейнера



2
Промежуточный
уровень
целостности
«Виртуализация»



2
Промежуточный
уровень
целостности
«Виртуализация»



>>>> Адаптированная контейнерная виртуализация

Защита контейнера от доступа на чтение



2
Промежуточный
уровень
целостности
«Виртуализация»



2
Промежуточный
уровень
целостности
«Виртуализация»



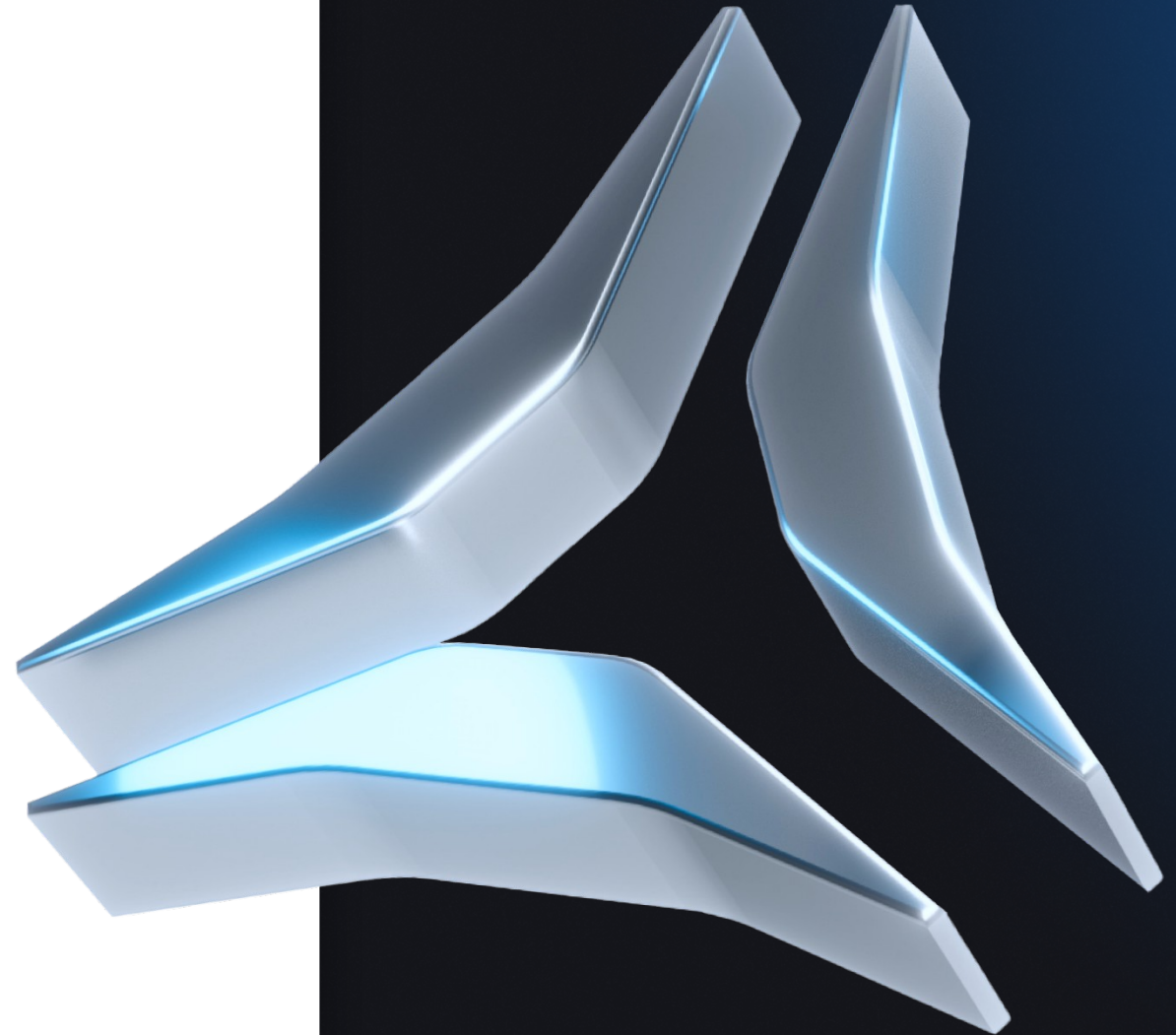
»»» Дальнейшие исследования

Развитие теоретической базы - разработка уровней МРОСЛ ДП-модели для средств контейнеризации

Интеграция со средствами оркестрации контейнеров и реализация в них МКЦ

Внедрение элементов ролевого управления доступом

Применение технологий ИИ (ML) для выявления аномалий в контейнерах





Спасибо!

Подписывайтесь
на наши обновления:

