Федеральное государственное образовательное бюджетное

учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Колледж информатики и программирования

**ОТЧЁТ**

**По практической работе**

**Практическая работа №4. «Мандатный контроль целостности в Astra Linux 1.6»**

**по дисциплине «Безопасность Astra Linux»**

Выполнил студент

Группы: 2ОИБАС-1222

Шишкин И. А.

Тизяков Е.Д.

Протасов Д.К.

Преподаватель

Сибирев И.В.

Оценка за работу :\_\_\_\_\_\_\_

**Москва – 2024г.**

**Мандатный контроль целостности в Astra Linux 1.6**

**Введение**

Мандатный контроль целостности (МКЦ) - это мощный механизм безопасности, который защищает систему от несанкционированных изменений и эксплуатации уязвимостей.

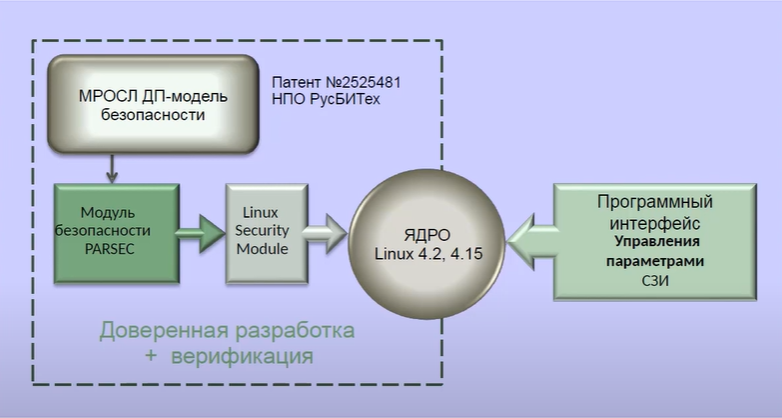
МКЦ реализован в Astra Linux 1.6 с помощью подсистемы безопасности Parsec.

**Теоретическое обоснование**

Дискреционное ограничение доступа (ДОС)\*\* контролирует доступ пользователей к файлам и другим ресурсам системы. Однако ДОС не позволяет управлять информационными потоками и предотвращать утечку данных.

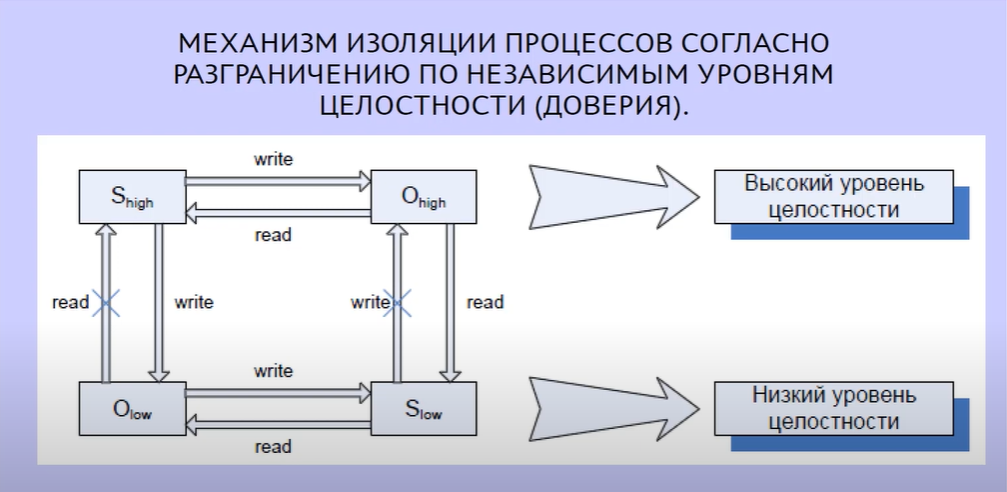
Мандатное управление доступом (МУД)\*\* вводит более детальные уровни контроля, основанные на уровнях конфиденциальности и категориях. МКЦ является частью МУД и дополняет его.

**Как работает МКЦ**



МКЦ использует концепцию уровней целостности. Объектам в системе (файлам, процессам и т.д.) присваиваются уровни целостности, которые определяют их важность для функционирования системы.

МКЦ не позволяет процессам с более низким уровнем целостности модифицировать объекты с более высоким уровнем целостности. Это предотвращает эксплуатацию уязвимостей в приложениях с более высоким уровнем целостности.



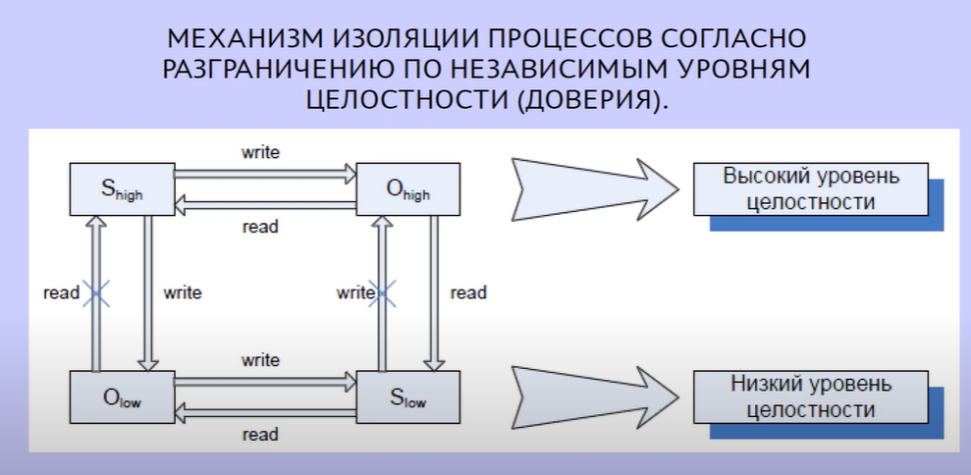
**Реализация в Astra Linux 1.6**

****

В Astra Linux 1.6 МКЦ используется для защиты приложений и их конфигурационных файлов.

Файлы изначально имеют максимальный уровень целостности.

Для включения МКЦ необходимо активировать защиту файловой системы в панели управления.



**Преимущества МКЦ**

Усложняет эксплуатацию уязвимостей нулевого дня.

Повышает безопасность системы путем управления информационными потоками.

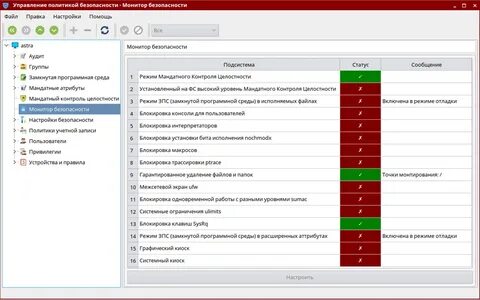
Усложняет проведение атак через взлом приложений.

**Мониторинг и защита от эксплоитов**



Монитор Parsec отслеживает действия процессов с низким уровнем целостности. Если обнаруживается попытка создания или запуска процесса с высоким уровнем целостности, Parsec прибивает такой процесс.

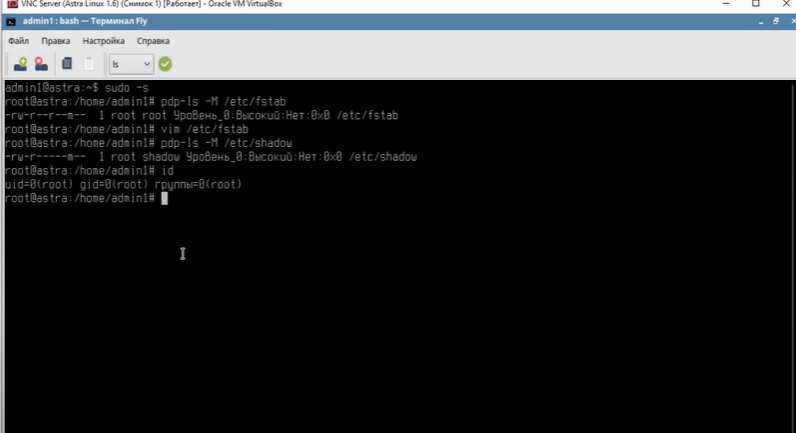
**Примеры работы МКЦ**



В Windows процессы с низким уровнем целостности не могут влиять на процессы с высоким уровнем, даже если они получают привилегии администратора.

В Astra Linux МКЦ защищает системные файлы и приложения от модификации неавторизованными пользователями или вредоносным ПО.

**Активация МКЦ**

****

Для активации МКЦ необходимо зайти в панель управления и включить защиту файловой системы.

После этого все файлы получат максимальный уровень контроля целостности.

**Ограничения МКЦ**

МКЦ не применяется к памяти и оперативной памяти.

Для внесения изменений в файлы с высоким уровнем целостности необходимо войти под соответствующим уровнем.

**Настройка МКЦ**

Уровни целостности и политики МКЦ можно настроить с помощью специальных утилит.

Рекомендации по настройке зависят от конкретной системы и приложений.

**Заключение**

МКЦ является важным инструментом защиты Astra Linux 1.6 от эксплойтов и несанкционированных изменений. Его использование значительно повышает уровень безопасности системы, делая ее устойчивой к различным атакам.