РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей

Презентация №10

Загружаемый модуль ядра macOS (Kext)

Студент: Эйвази Мани

Группа: НПИбд-03-24

Студенческий билет №: 1032245107

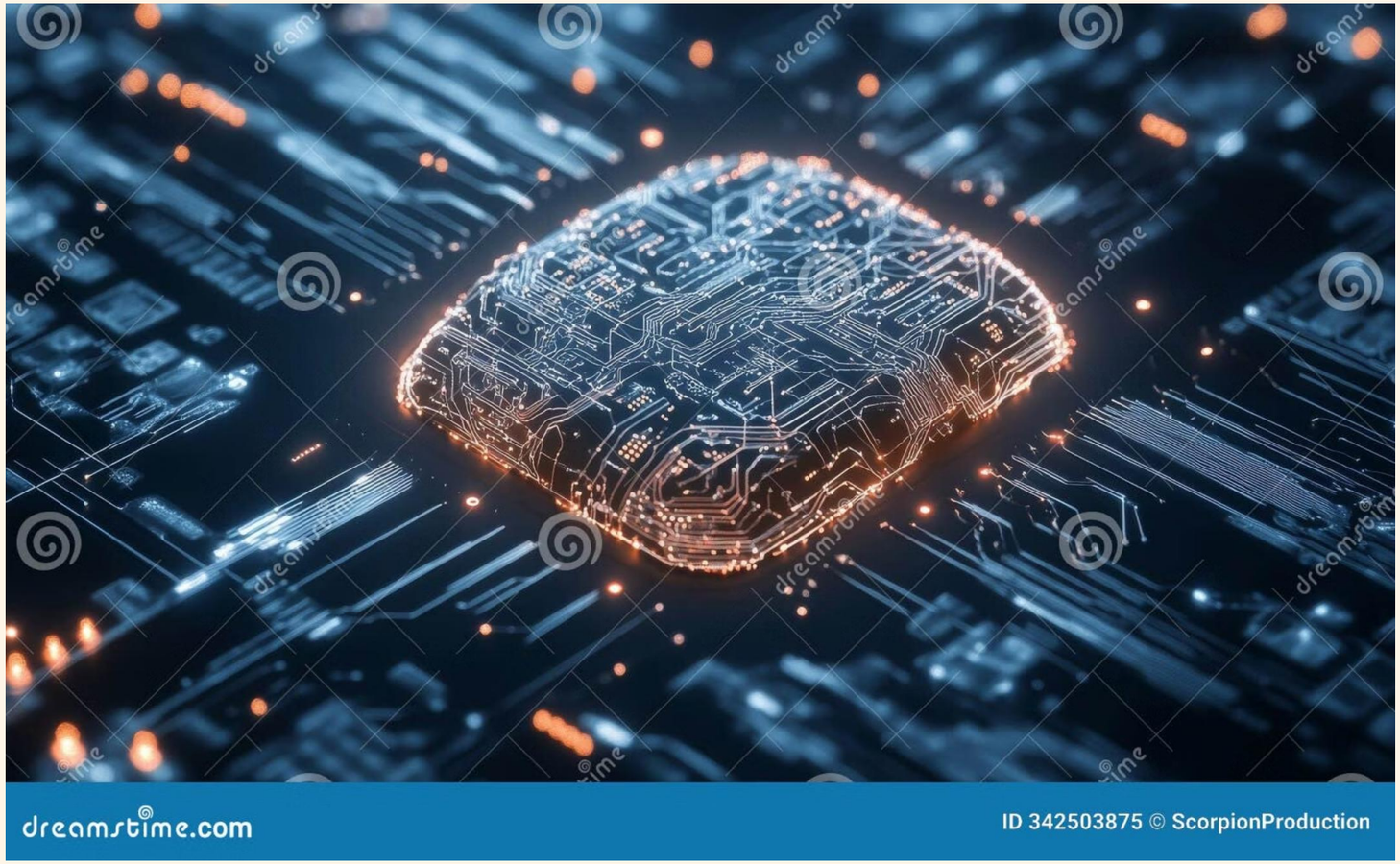
Загружаемый модуль ядра macOS (Kext)

Обзор архитектуры, назначения и эволюции Kernel Extensions в macOS

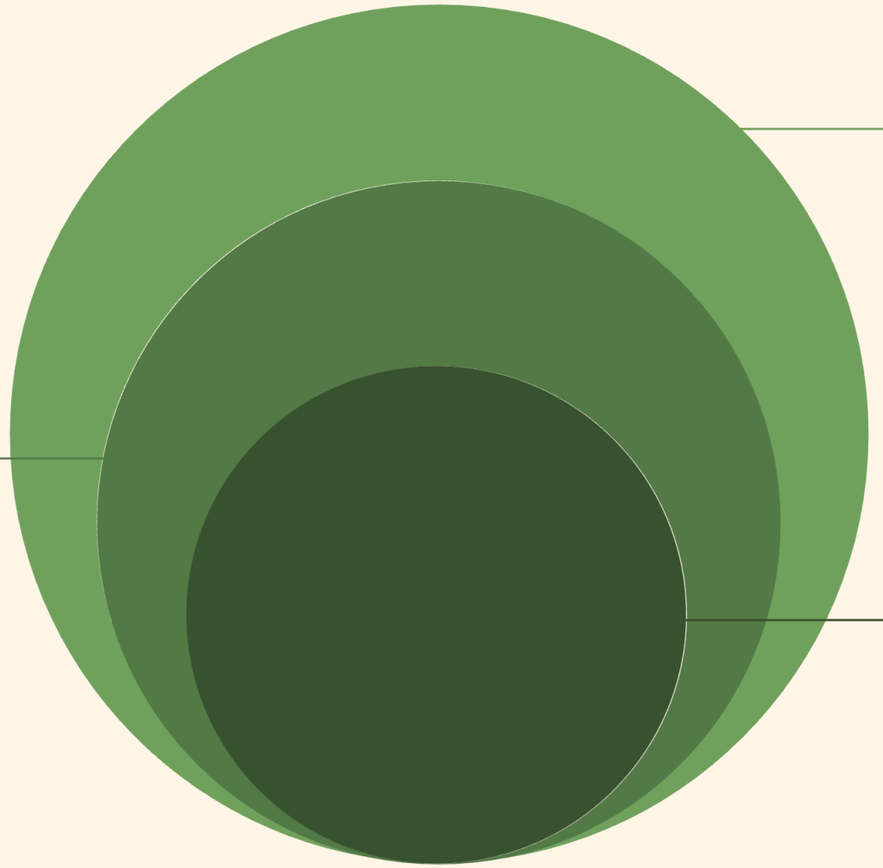
Kext: Определение и Назначение

Kernel Extension (kext) — это динамически загружаемый модуль кода, который расширяет функциональность ядра macOS.

- *Позволяет добавлять новые функции в ядро системы без его полной перекомпиляции.*
- *Используется для создания драйверов устройств (например, сетевых карт, USB-устройств).*
- *Предоставляет интерфейсы для взаимодействия оборудования с операционной системой.*



Архитектура XNU и Место Kext



I/O Kit & Kext

Объектные драйверы и взаимодействие kext

Слой BSD

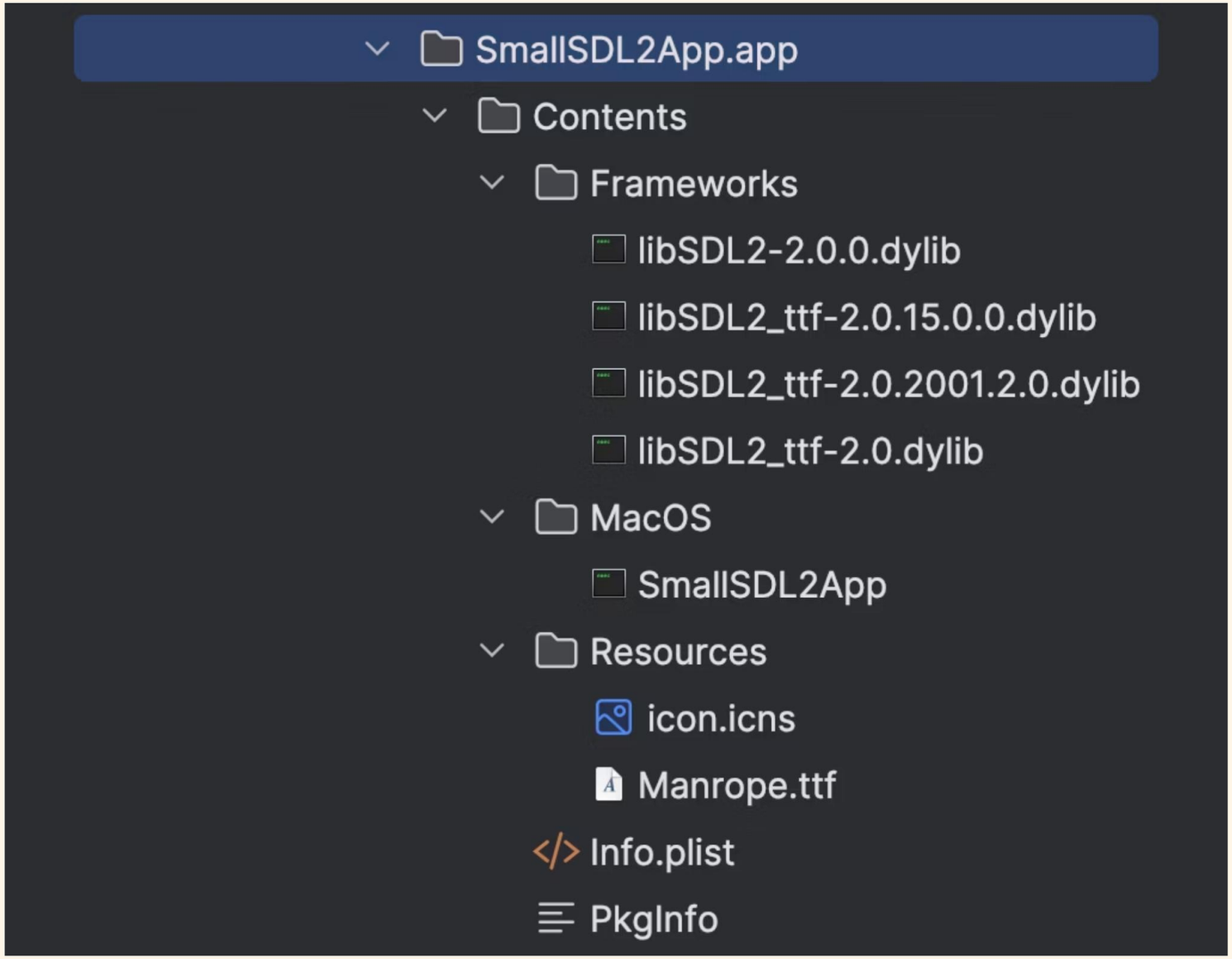
Процессы, файловая система и сеть

Ядро Mach

Микроядро, управление задачами и IPC

Ядро XNU, основа macOS, состоит из микроядра Mach и слоя BSD. I/O Kit предоставляет объектно-ориентированную среду для разработки драйверов, где kext занимает центральное место.

Структура Kext: Формат и Расположение



Kext представляет собой бандл — специальную директорию с расширением `.kext`*, содержащую исполняемые файлы, ресурсы и файл* `Info.plist`*.*

- ***/System/Library/Extensions:*** *Системные kext.*
- ***/Library/Extensions:*** *Kext сторонних разработчиков.*
- *Kext кэшируются для ускорения загрузки и повышения производительности.*

Жизненный Цикл Kext: Управление

01

Загрузка (kextload)

Команда `kextload` *используется для загрузки kext в ядро.*

02

Проверка (kextutil)

`kextutil` *проверяет kext на соответствие требованиям и может выполнять отладку.*

03

Статус (kextstat)

`kextstat` *отображает список загруженных kext и их статус.*

```
# kextstat | grep -v com.apple
```

04

Выгрузка (kextunload)

Команда `kextunload` *позволяет удалить kext из ядра.*

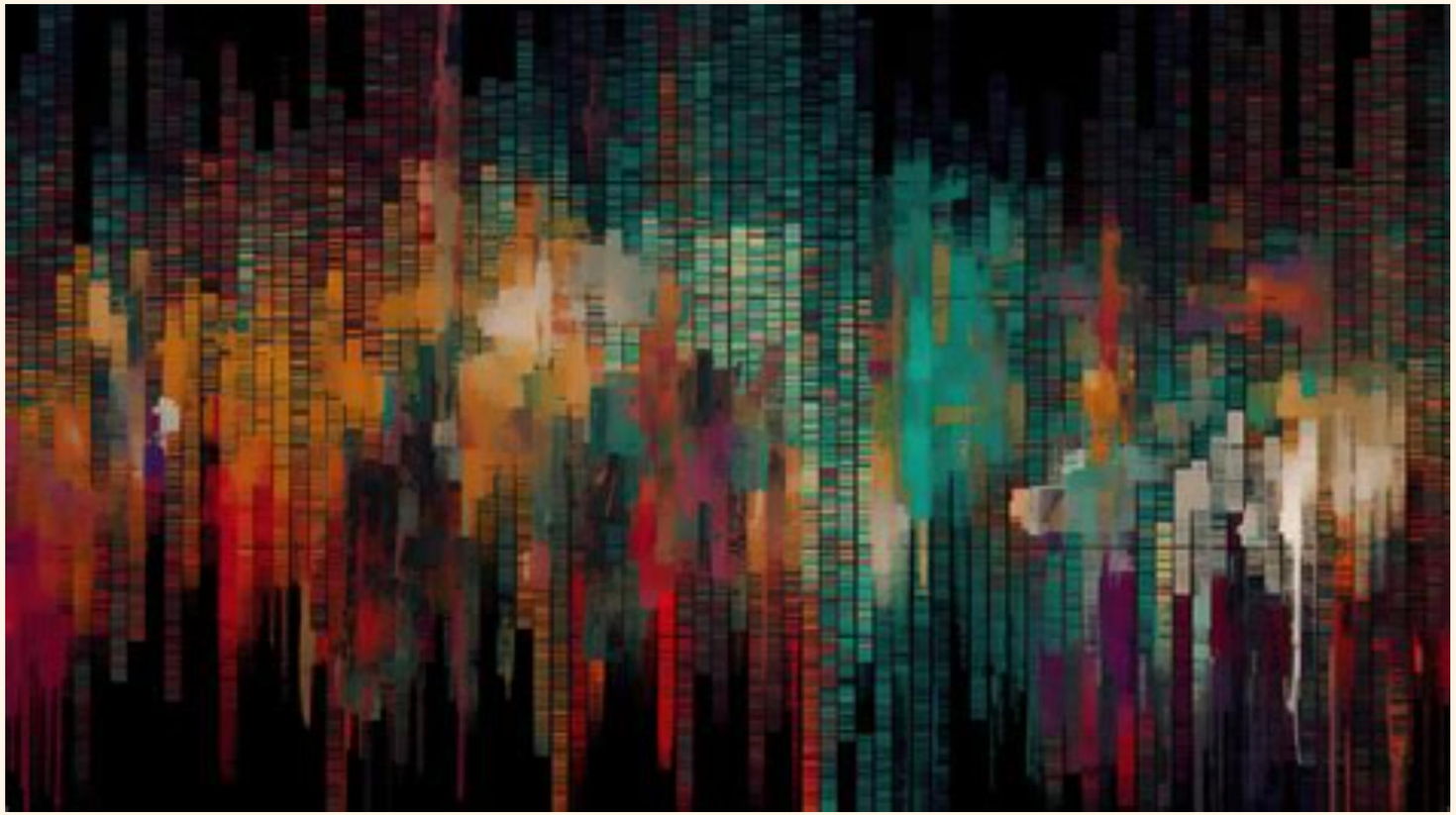
Проблемы Kext: Безопасность и Стабильность

Сложность Разработки

- *Разработка kext требует глубоких знаний ядра.*
- *Ошибки могут привести к серьезным сбоям системы.*

Риски для Безопасности

- ***Kernel Panic:***
- *Уязвимости в kext могут быть использованы для повышения привилегий.*



Ограничения Загрузки Kext

System Integrity Protection (SIP)

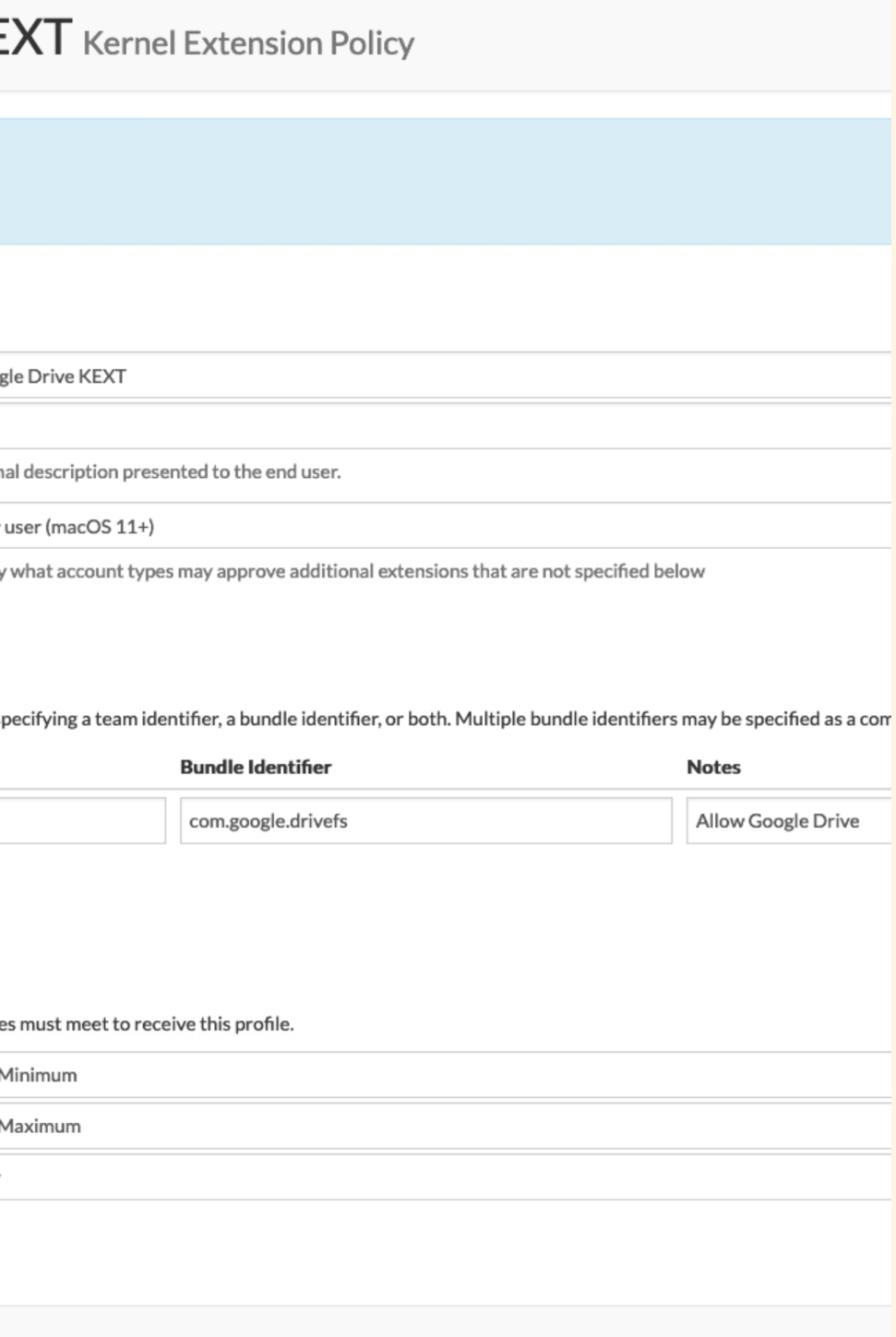
SIP блокирует модификацию системных файлов и защищает критические области, включая директории с kext.

Подпись Кодов

Все kext должны быть подписаны сертифицированным разработчиком Apple для загрузки в macOS High Sierra и новее.

MDM и Управление

Mobile Device Management (MDM) позволяет удаленно утверждать и управлять загрузкой kext в корпоративных средах.



Новая Архитектура: System Extensions и DriverKit

Начиная с macOS Catalina, Apple активно продвигает замену kext на более безопасные и современные технологии: System Extensions и DriverKit (dext). Это стратегический шаг к повышению стабильности и безопасности системы.

Kext vs. Dext: Ключевые Отличия

Среда выполнения	*Ядро операционной системы*	*Пользовательское пространство (вне ядра)*
Язык разработки	*C++ (I/O Kit)*	*Swift, Objective-C (с KEXT-подобным API)*
Безопасность	*Высокие риски (kernel panic, уязвимости)*	*Изоляция от ядра, повышенная стабильность*
Отладка	*Ограниченные возможности*	*Стандартные инструменты Xcode*
Влияние на систему	*Может вызвать нестабильность всей ОС*	*Ошибки затрагивают только сам процесс dext*

Заключение: Будущее Расширений Ядра macOS

Kext: Deprecated

Apple активно сокращает поддержку kext. В будущих версиях macOS их использование будет полностью прекращено.

Миграция на System Extensions

Разработчикам рекомендуется переносить функционал своих kext на System Extensions и DriverKit для совместимости.

Безопасное Будущее

Новые технологии обеспечивают значительно более высокий уровень безопасности и стабильности системы macOS.

Спасибо за внимание