ИТМО

Информационная безопасность в архитектуре SDN

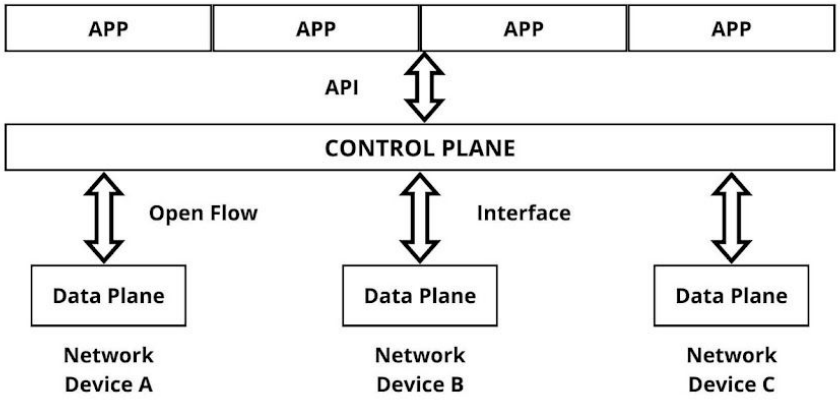
Выполнил: Исламов Сергей K34202

Введение

ИТМО

- SDN – это новый подход к управлению сетями, который обеспечивает гибкость и автоматизацию.

Архитектура SDN



WEP

Угрозы безопасности

- Атаки на контроллер (DDoS, перехват API)
- Подмена таблиц маршрутизации (Flow Table Overflow)
- Перехват управляющих команд (MITM-атака)
- Компрометация SDN-приложений

Методы защиты

- Шифрование связи (TLS, IPsec)
- Контроль доступа
- Мониторинг трафика и аномалий (AI/ML)
- Защита API (OAuth, JWT)
- Автоматизированное реагирование на атаки

AI/ML

ИТМО

- Анализ трафика в реальном времени
- Предсказание атак с помощью машинного обучения
- Самовосстанавливающиеся сети (Self-Healing Networks)
- Автоматизированное блокирование атак
- Интеллектуальные IDS/IPS

Заключение

SDN упрощает управление сетями, а также позволяет использовать уникальные методы защиты. Для защиты рекомендуется использовать:

1. **Шифрование и аутентификация соединений.**
2. **Мониторинг аномалий с использованием AI.**
3. **Изоляция критически важных элементов SDN.**
4. **Гибридные модели безопасности с блокчейном и Zero Trust.**

Безопасность SDN – это активная область исследований, и в будущем ожидается развитие интеллектуальных решений для защиты сетевых инфраструктур.

Спасибо
за внимание!

ITMO more than a UNIVERSITY