Микроядерная ОС:
Преимущества и реальные сценарии

Иван Воробьев

Менеджер по сопровождению ключевых
корпоративных проектов, Лаборатория Касперского

kaspersky

Почему микроядро?

96%

критических уязвимостей Linux перестают быть таковыми в микроядерной операционной системе

57%

уязвимостей перейдут в категорию низкого уровня опасности в ОС в микроядерном исполнении

29%

эксплойтов можно полностью предотвратить без верификации в микроядерной ОС

«С точки зрения безопасности монолитная архитектура ОС изначально уязвима и является корневой причиной большинства случаев компрометации. Поэтому пора переходить к структуре ОС, которая более адекватно отвечает требованиям безопасности XXI века»

Таненбаум — Торвальдс

Источник: Simon Biggs, Damon Lee, Gernot Heiser. 2018. The Jury Is In: Monolithic OS Design Is Flawed: Microkernel-based Designs Improve Security

Что такое KasperskyOS?

Микроядерная операционная система для отраслей с повышенными требованиями к информационной безопасности

Микроядро

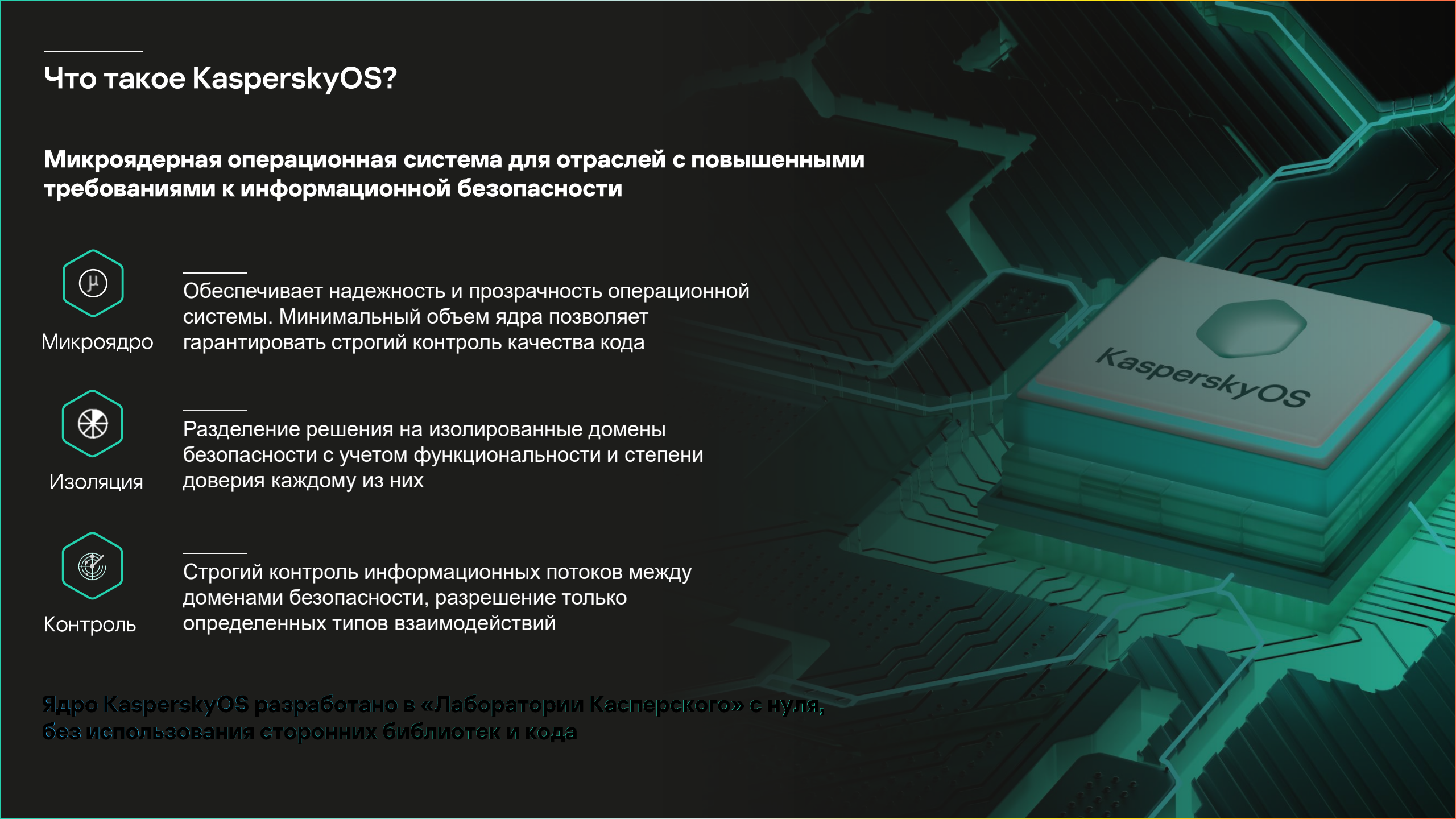
Обеспечивает надежность и прозрачность операционной системы. Минимальный объем ядра позволяет гарантировать строгий контроль качества кода

Изоляция

Разделение решения на изолированные домены безопасности с учетом функциональности и степени доверия каждому из них

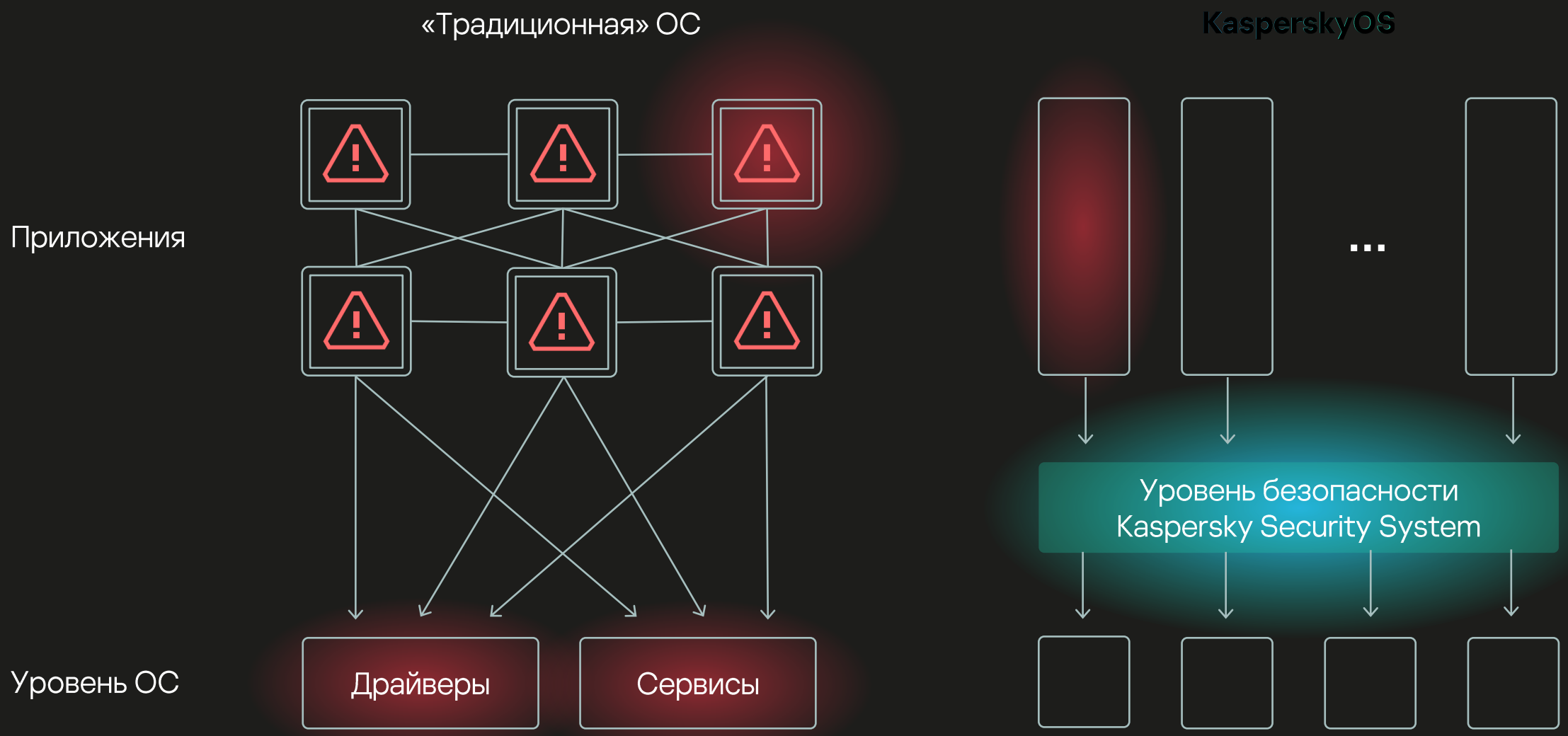
Контроль

Строгий контроль информационных потоков между доменами безопасности, разрешение только определенных типов взаимодействий



Ядро KasperskyOS разработано в «Лаборатории Касперского» с нуля, без использования сторонних библиотек и кода

KasperskyOS: основные отличия от традиционных ОС



Области применения кибериммунных продуктов

Шлюзы для защиты IoT, включая индустриальный

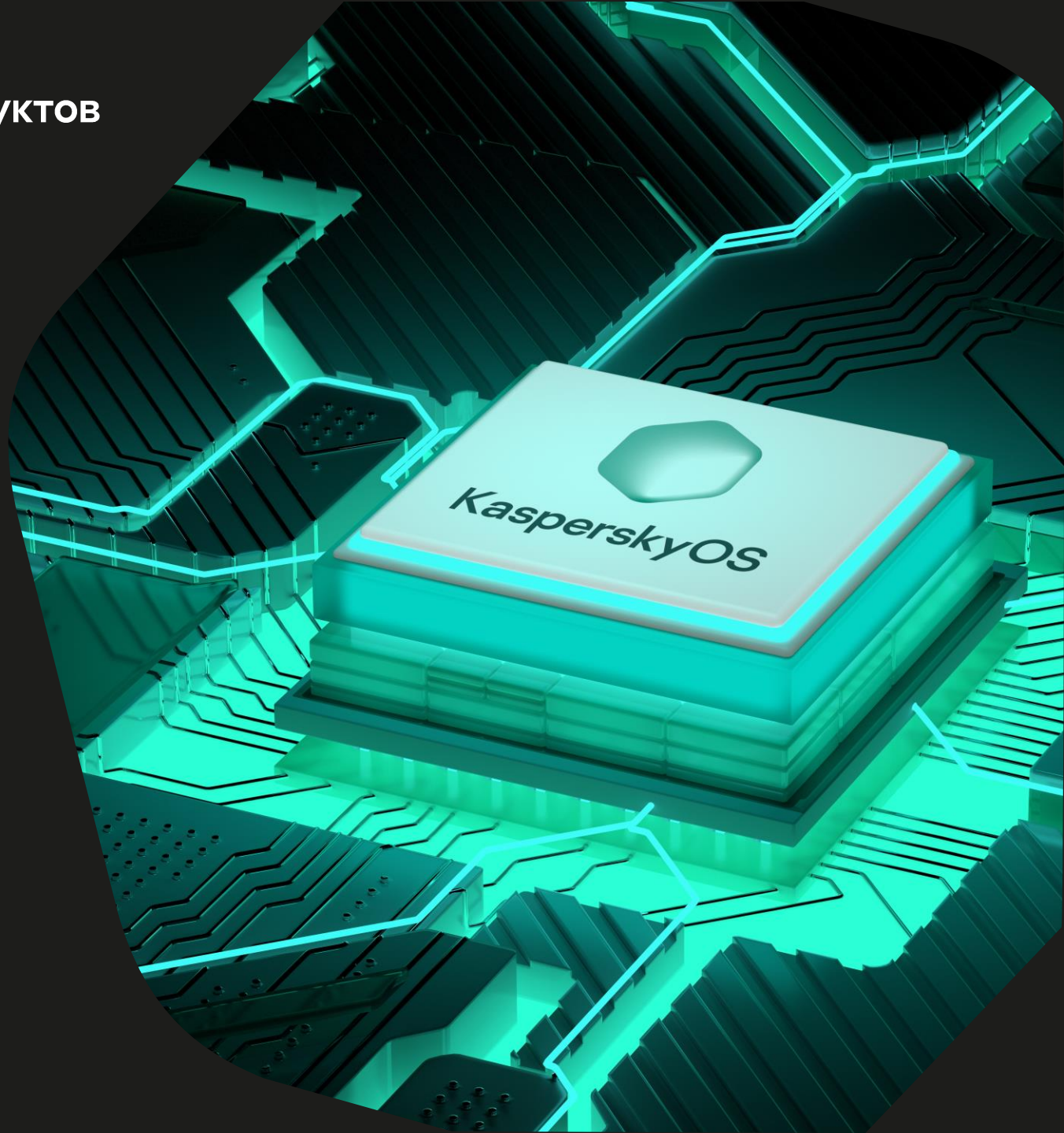
Инфраструктура виртуальных рабочих столов

Профессиональные мобильные устройства

Электронные блоки в составе умных автомобилей

Контроллеры в IT-системах умных городов

Доверенная среда исполнения



Решения на базе KasperskyOS обладают **«встроенной» защитой от кибератак**. Они выполняют свои критические функции даже в условиях агрессивной внешней среды **без дополнительных (наложенных) средств безопасности**

Программно-аппаратные комплексы на базе KasperskyOS

Kaspersky
IoT Secure Gateway

aprotech Kaspersky IoT company

Kaspersky
Thin Client

TONK

Готовые решения

Kaspersky
Professional Mobile
Platform

Исследовательские
проекты

Кибериммунные шлюзы для защиты интернета вещей

Система обнаружения и предотвращения вторжений (IDS / IPS) с сертификатом ФСТЭК** ИТ.СОВ.С4.ПЗ

Межсетевой экран
с сертификатом ФСТЭК* ИТ.МЭ.Д4.ПЗ

Поддержка VPN**
(Client-to-Site & site-to-site) с сертификатом ФСБ (СКЗИ по классу КС2)

TCP / IP маршрутизатор
(3G / LTE роутер)

2 режима работы
Двунаправленная передача данных (МЭ);
Программный дата-диод (конвертер)

Edge Computing Platform
Платформа для портирования приложений

Конвертация промышленных данных:
Из OPC UA / ModBus TCP в MQTT / МЭК 104;
Универсальный конвертер протоколов

Анализ промышленных протоколов:
Фильтрация сигналов и команд;
Контроль допустимых значений;
Network Protector

Отказоустойчивая конфигурация шлюза:
VRRP-кластеризация

Централизованное управление и мониторинг через KSC:

Классификация устройств в сети*
(Device Detection)

Port Forwarding (NAT)
Статическая маршрутизация

* Реализация в 2024 г.
** Реализация в 2025 г.

Режим работы KISG

Основной функционал KISG	ДИОД	МЭ
		
Транспорт данных	• Однонаправленный: Ethernet, 3G/LTE	• Двунаправленный: Ethernet, 3G/LTE
Сетевые функции	• DHCP сервер	• DHCP сервер • Настройка статических маршрутов • NAT и PAT (Port Forwarding) • VRRP • MQTT брокер
Поддержка сторонних приложений (Edge Computing)	• Приложения конвертера протоколов: • OPC UA Client / Modbus TCP (**LAN**) • MQTT Publisher (**WAN**)	• Поддержка серверных приложений в 2025 • (Modbus TCP Server, OPC UA Server - **WAN**)
Безопасность	• Шифрованный канал TLS • VPN Client (VipNet Client)	• Межсетевой экран (Default Deny) • Контроль и фильтрация промышленных протоколов (MQTT, Modbus, BACnet, DNP3, MMS, OMRON-FINS, ENIP/CIP, TriStation, S7comm) • IDS/IPS – модуль обнаружения и предотвращения сетевых вторжений • DPI – Фильтрация (блокирование) трафика прикладных протоколов: FTP, HTTP, MQTT, Modbus, SMTP, IMAP, POP3
Сертификация	• ФСТЭК ИТ.ОС. А4.ПЗ (ОС типа «А» 4-го класса) • ГОСТ VPN по СКЗИ КС1 и КС2 (2025 г.)	• ФСТЭК ИТ.ОС. А4.ПЗ (ОС типа «А» 4-го класса) • ФСТЭК ИТ.МЭ.Д4.ПЗ (тип «Д» 4-го класса)
Гибкое управление шлюзом	• Централизованное управление через KSC • Веб-интерфейс • Управление доступом на основе ролей • Интеграция с SIEM	
Защита шлюза от кибератак	• Кибериммунитет (Secure by design) • Безопасная загрузка (Secure boot) • Безопасное обновление (Secure update)	

Безопасное подключение к удаленным рабочим столам

Kaspersky Thin Client (KTC) — решение для построения кибериммунной инфраструктуры тонких клиентов с удобным централизованным управлением

РУТОКЕН BASIS TONK АЙТИБАСТИОН Аладдин SafeNet

Защита на уровне ОС
Тонкие клиенты на базе KasperskyOS обладают кибериммунитетом — «врожденной» защищенностью на уровне архитектуры ОС

Единый центр управления
Удобное централизованное управление тонкими клиентами для ИТ- и ИБ-специалистов

Совместимость
Возможность подключения к системам виртуализации рабочих мест

Экономия
Снижение затрат на развертывание и обслуживание инфраструктуры тонких клиентов благодаря централизованному управлению

Соответствие нормативам
Продукты в составе решения соответствуют приказу Минкомсвязи России о преимущественном использовании отечественного ПО

Компоненты в составе решения выполняют требования Минцифры и входят в реестр российского ПО: KISG 100 №248061 от 06.12.2021 и KISG 1000 №11928 от 29.10.2021

Сценарии применения: рабочие станции инженеров

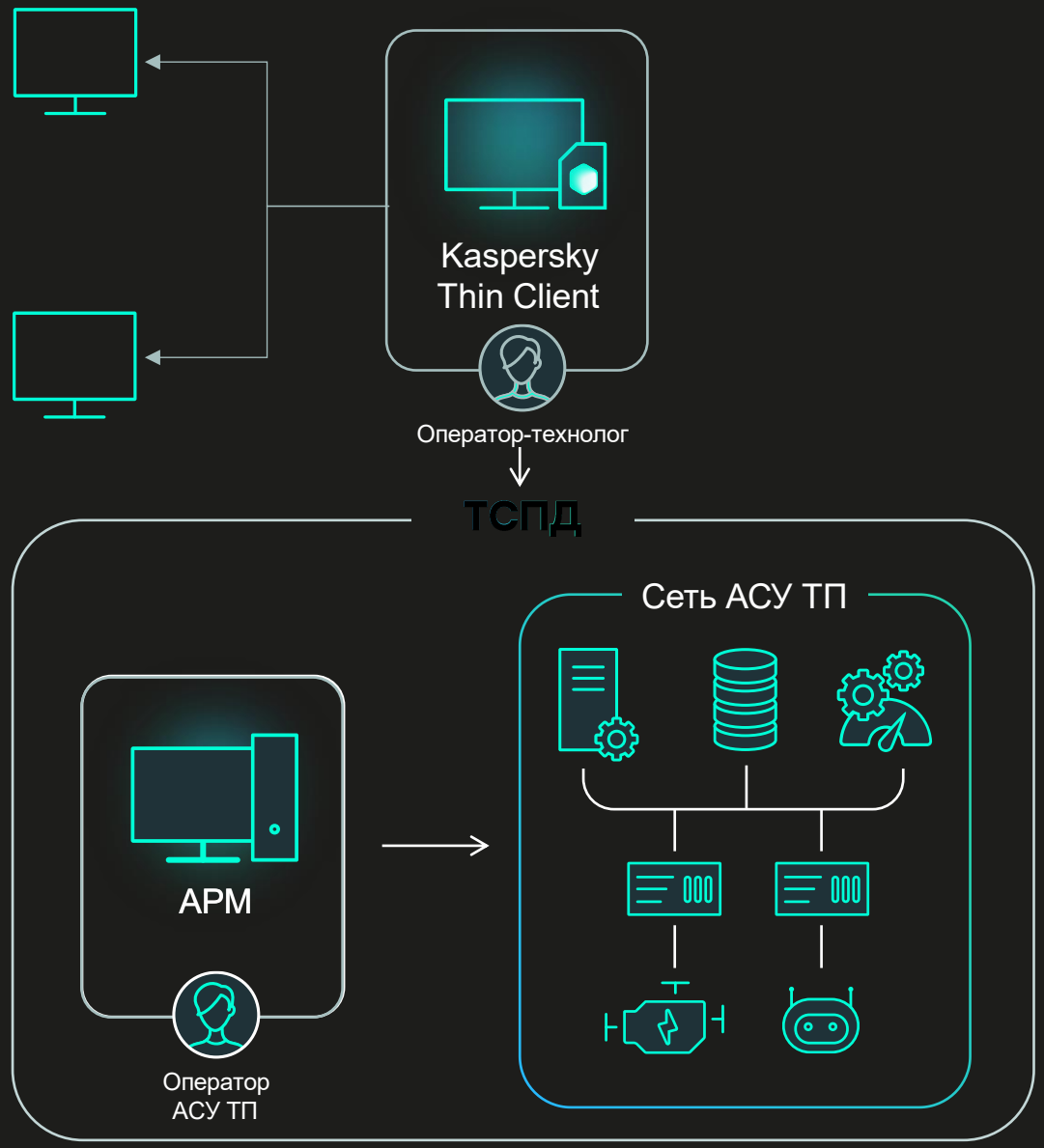
Типы задач оператора

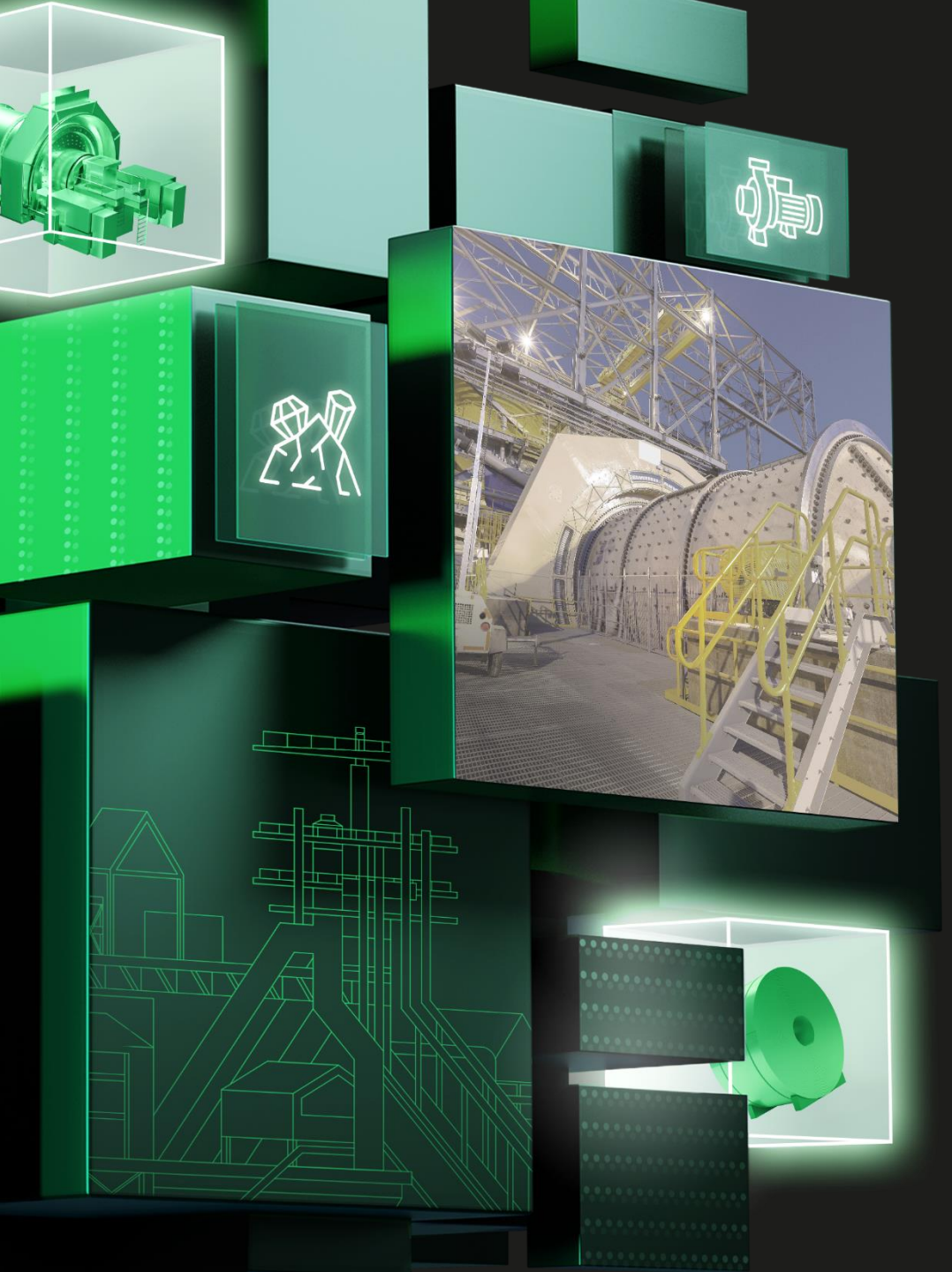
Операторские и инженерные станции, которые подключены к SCADA-системе или к станкам на производстве

Средства отображения HMI/информационные панели

- Мониторинг промышленных процессов в реальном времени
- Режим ограниченной функциональности (kiosk)

Энергетика
и производство





Спасибо!