АБИСС

# О процессах сертификации решений для КИИ

Поликарпов Александр
Старший системный аналитик
АО «Лаборатория Касперского»

# Постановка задачи

**Импортозамещение устройств класса «Межсетевой экран типа Д»:**
**Cisco, Sierra Wireless, Huawei, Moxa, Check Point, Fortinet, Trend Micro**

**ТРЕБОВАНИЯ ДЛЯ ИНТЕГРАЦИИ В КИИ:**

**ПРОФИЛЬ ЗАЩИТЫ МЕЖСЕТЕВЫХ ЭКРАНОВ ТИПА «Д» ЧЕТВЕРТОГО КЛАССА ЗАЩИТЫ ИТ.МЭ.Д4.ПЗ**

**ПРОФИЛЬ ЗАЩИТЫ ОПЕРАЦИОННЫХ СИСТЕМ ТИПА «А» ЧЕТВЕРТОГО КЛАССА ЗАЩИТЫ ИТ.ОС.А4.ПЗ**

**ПРИКАЗ №239 ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ, УСТАНАВЛИВАЮЩИЕ УРОВНИ ДОВЕРИЯ К СРЕДСТВАМ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И СРЕДСТВАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»**

# Этапы работ

Предварительная этап

Сертификация

сентябрь – ноябрь 2022

ноябрь 2022 – январь 2023

январь 2023 – декабрь 2023

2024

Подготовка материалов

Анализ реализации на соответствие требованиям

Доработка кодовой базы для соответствия требованиям

Сертификационные испытания

**Предоставление информации о целевых функциях продуктов, их внедрения в предполагаемую инфраструктуру заказчика**

**Подготовка материалов с описанием предполагаемой реализации мер защиты**

**Уточнение реализации функциональных компонент, обеспечивающих выполнение требований.**

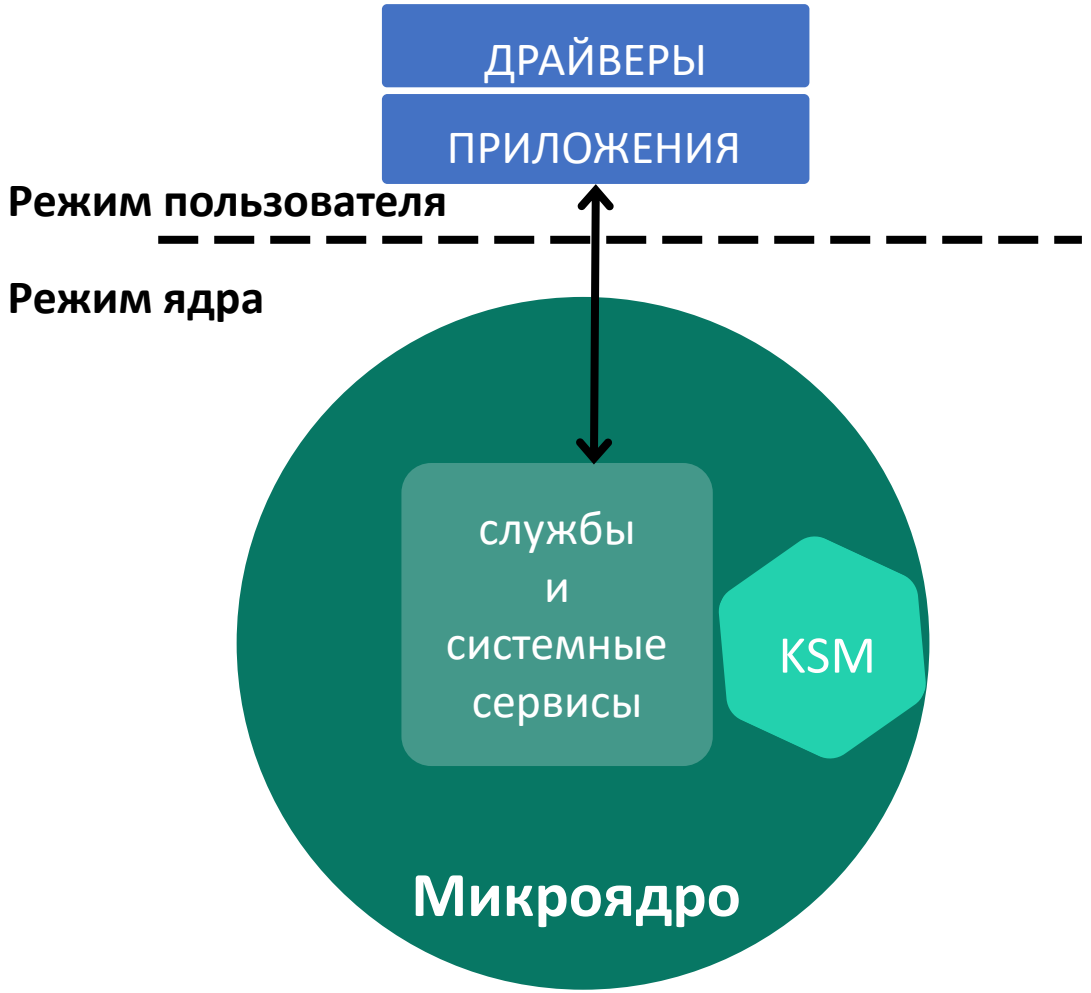
**Подготовка документации**

# Предварительный этап

Подключение ИЛ «Фобос-НТ»* к работе по формированию требований на доработку кодовой базы

**Специфика объекта оценки:**

- Микроядерная архитектура ОС
- Разделение на домены безопасности (MILS)
- Запрет любых действий не предопределённых политиками безопасности
- Отсутствие ролевой модели и понятия «пользователь»
- Отсутствие механизмов аутентификации




*Реестр аккредитованных ФСТЭК России испытательных лабораторий

# Доработка кодовой базы

- Интеграция ролевой модели в политики безопасности - Static RBAC 
- Двухфакторная аутентификация пользователей 
- Контроль целостности исполняемых файлов с использованием криптографических алгоритмов 
- SDL – фаззинг, статический и динамический анализ компонент доверенной кодовой базы

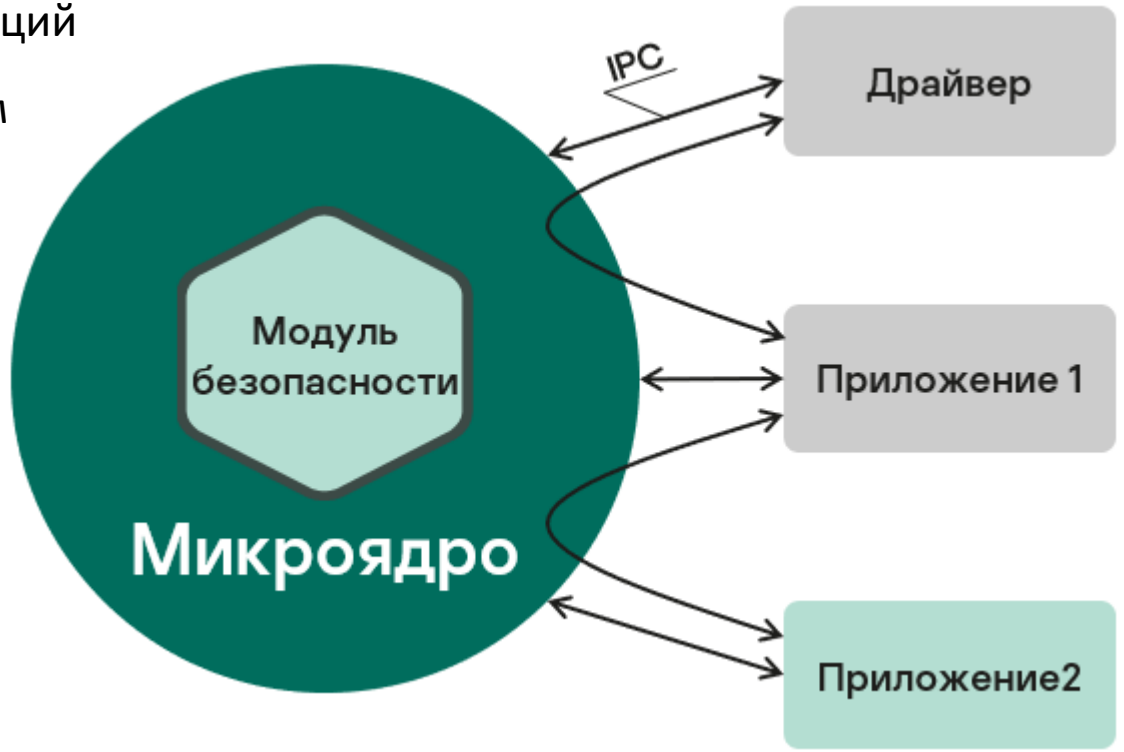
***Сформирована «поверхность атаки»***

***Определена необходимость разработки формальной модели для реализуемых политик безопасности***

***Привлечение ИЛ  на ранних этапах разработки позволяет снизить риски масштабных изменений сертифицируемых продуктов***

# Формальная модель TLA+

(temporal logic of actions) – язык спецификаций для описания свойств и поведения систем

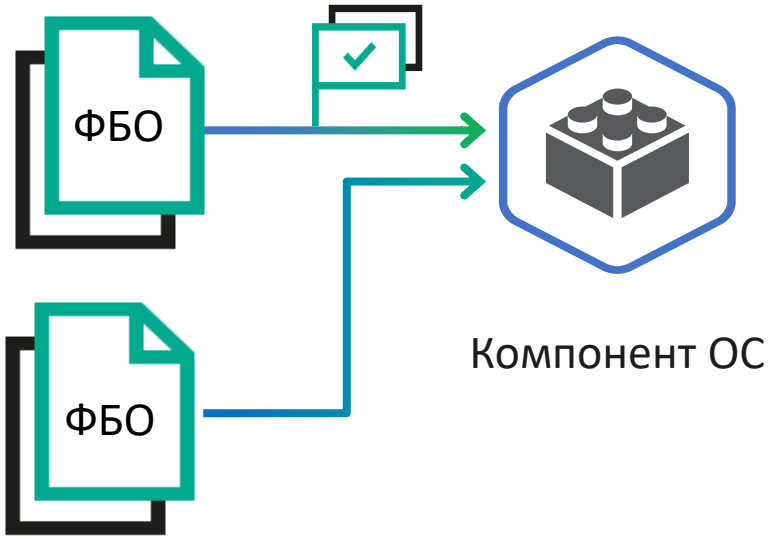


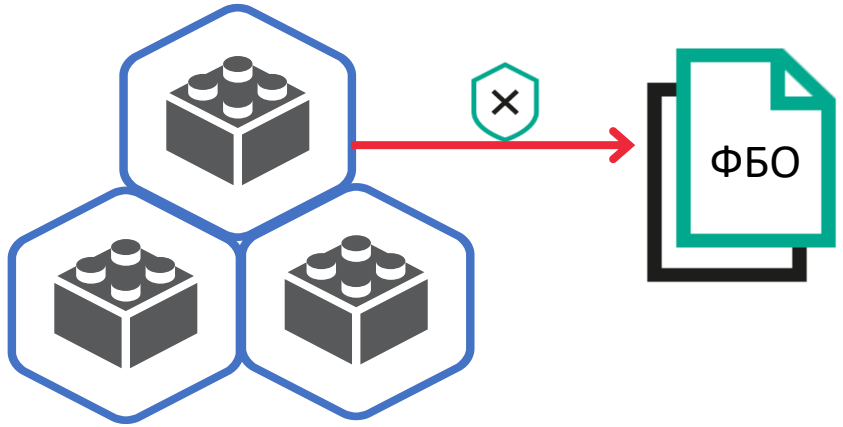

Формулирует свойства **непротиворечивости** и **консистентности**, которые проверяются автоматически с помощью инструмента проверки моделей **TLC**

Любые вызовы в политике безопасности должны быть ассоциированы с пользователем, определены атрибуты (чтение\запись)

# Реализация функций безопасности компонентами ОС






**Сложность оценки и планирования** - интеграция компонента в общее решение, т.к. нужно определить поведение некоторой абстрактной программной реализации

**Концепция:**
На один сценарий реализуется один компонент (законченный программный модуль),
если есть несколько похожих сценариев, то расширяем реализацию компонента на несколько сценариев.
Обратного решения не допускаем, то есть один сценарий не может быть реализован несколькими программными компонентами.

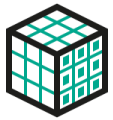
**Преимущества:**

Возможность вести разработку компонента и проверку всех необходимых тестовых сценариев функциональности одному или нескольким исполнителям без постоянной синхронизации со смежными командами (реализующими другие компоненты);

Для испытательной лаборатории такая концепция позволяет более четко понимать границы компонентов, реализующих функции безопасности, рассматривать все решение как совокупность таких компонентов.
Для каждого компонента ФБО можно создать полный перечень тестовых воздействий, описывающих позитивные и негативные сценарии его поведения;

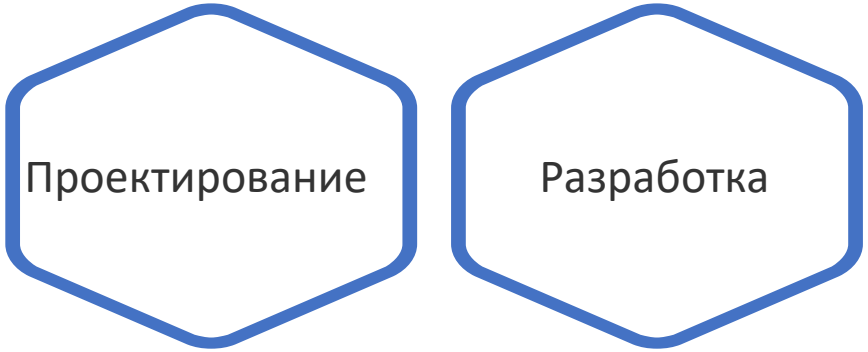
На этапе анализа ПО так же упрощается каталогизация и анализ модулей, непосредственно входящих в компонент ФБО.

**Недостатки:**



Значительные изменения архитектуры решения

## Операционная безопасность ПО



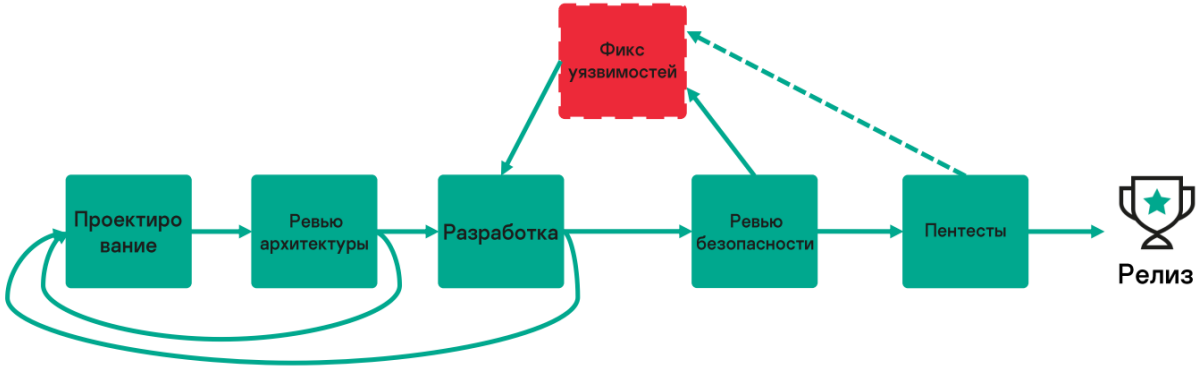

ИБ-ревью для обеспечения безопасности разработки, выявление уязвимостей ПО, проверка явного нарушения целостности, доступности и конфиденциальности...

Пентесты — тесты на проникновение (penetration tests), имитация реального взлома системы.

**Недостатки:**

Множество итераций изменения ПО

## Secure by design




Добавляется этап ревью архитектуры.
Оценка соответствия архитектуры паттернам (методологии, требованиям).

**Преимущества:**

Баги, найденные на стадии разработки удастся исправить без значительного изменения ПО

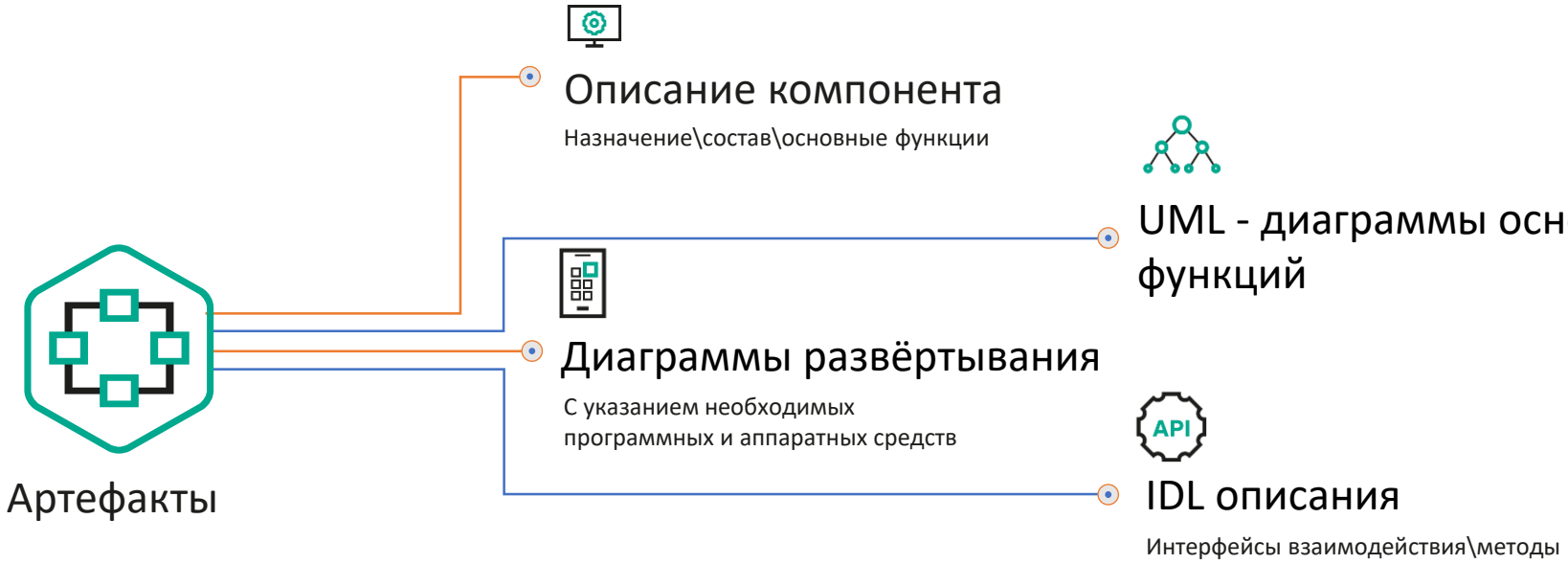
*чтобы работа с багами не превратилась в бесконечное шествие по кругу, в проекте нужен эксперт по безопасности, который будет выявлять проблемы на всех стадиях разработки.*

## **Secure by design** — проектирование с учетом заложенной безопасности

- **Концептуальная целостность**

- **Непротиворечивость**

*Архитектурный комитет - «Группа людей, специализирующихся в своих областях, представляющих свои интересы, принимающих общесистемное архитектурное решение.»*



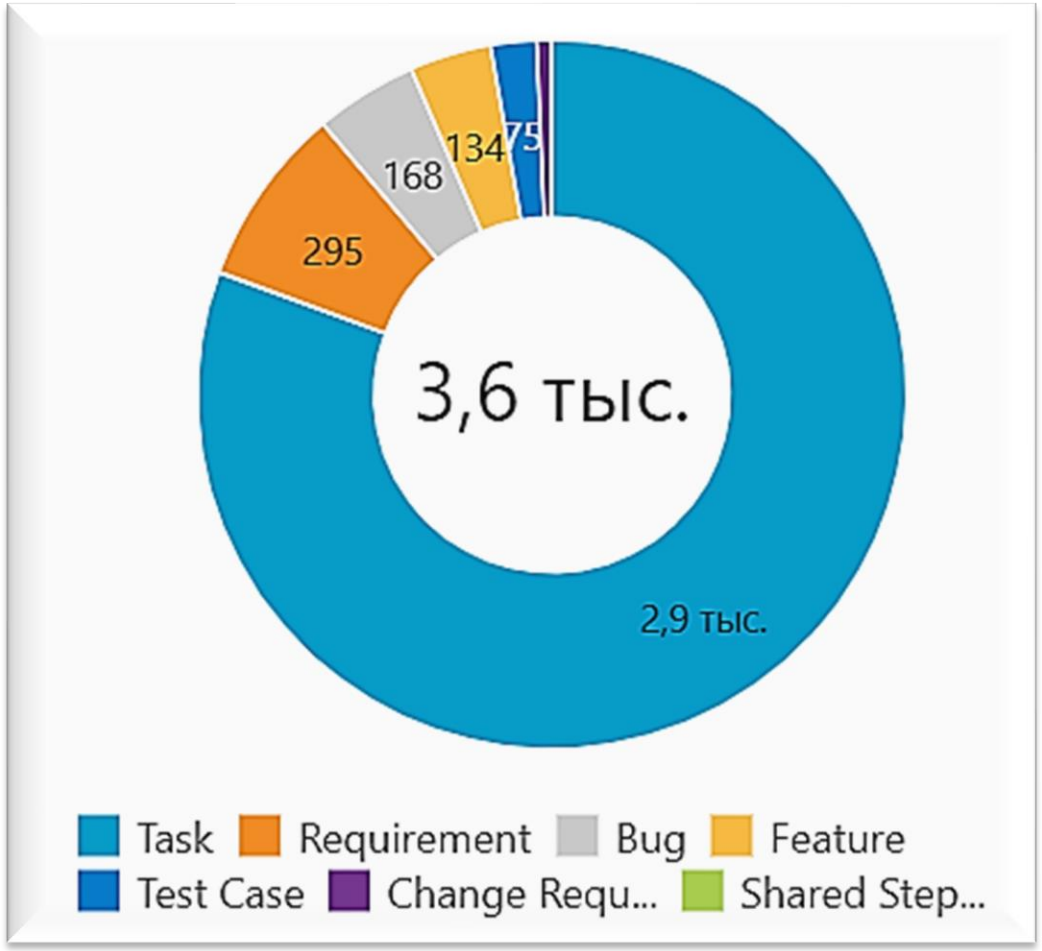
## Декомпозиция работ

- Требования ФБО = Requirement

**Пример: Authenticator**

- 26 Требований – 1 компонент ОС

System analyst




Наполнение требования понятным для разработчика (программиста) набором "элементов действия" (action items) — задокументированное событие, задача или действие, которое необходимо выполнить.

# Внедрение практик SDL

Базовый уровень зрелости бизнес-процессов

**Фаззинг**

Code coverage – 80%

*Для компонентов на «поверхности атаки»*

Метрики ФСТЭК по УД4

**Динамический анализ**

Интеграция санитайзеров (AddressSanitizer; UndefinedBehaviorSanitizer) в сборку с компонентами «доверенной кодовой базы»

**Статический анализ**

Статический анализатор «Svace» – интеграция в конвейер, устранение критических «срабатываний» (major, critical)

***Фикс багов и уязвимостей на раннем этапе. Снижение затрат на релизе продукта***

**ГОСТ. Р 56939-2016**

# *Ограничения — двигатель прогресса*

**Выводы:**

- Разработка и интеграция компонентов, реализующих функции безопасности, в «доверенную кодовую базу» с возможностью переиспользования в различных продуктах;
- Снижение стоимости (сроков) разработки с использованием подхода secure by design;
- Унификация решений, реализующих функции безопасности и запросы бизнеса;
- Получение компетенций о процедурах и требованиях регуляторики широким кругом исполнителей.

# Вопросы?

**Александр Поликарпов |** Старший системный аналитик | KasperskyOS Team **|** Kaspersky
Office: +7 495 797 8700 | Mobile:+7 977 845 11 25 | Alexander.Polikarpov@kaspersky.com
Business Centre “Olimpia Park”, 39A/3 Leningradskoe Shosse, Moscow, 125212, Russia | os.kaspersky.com | www.kaspersky.com
**KasperskyOS. Be immune.**

kaspersky 25 years DREAM TEAM. REAL PEOPLE.