Лаборатория Касперского: новые подходы в безопасности корпоративной ИТ-инфраструктуры

kaspersky

Отвечаю за enterprise портфолио Лаборатории Касперского

Образование:
- ✓ СПб ГУТ им. проф. М.А. Бонч-Бруевича (многоканальные телекоммуникационные системы)
- ✓ Университет ИТМО (информационная безопасность)

Опыт:
- ✓ техническая защита информации и ПДИТР
- ✓ проектирование и внедрение систем защиты информации

с 2018 г. в Лаборатории Касперского

Александр Комиссаров

Инженер предпродажной поддержки
Alexander.Komissarov@kaspersky.com
+7 (969) 730 89 30
linkedin.com/in/alexander-komissarov

Содержание

Цифровое голосование Polys

Известные проблемы онлайн-голосований

Подмена голосов избирателей

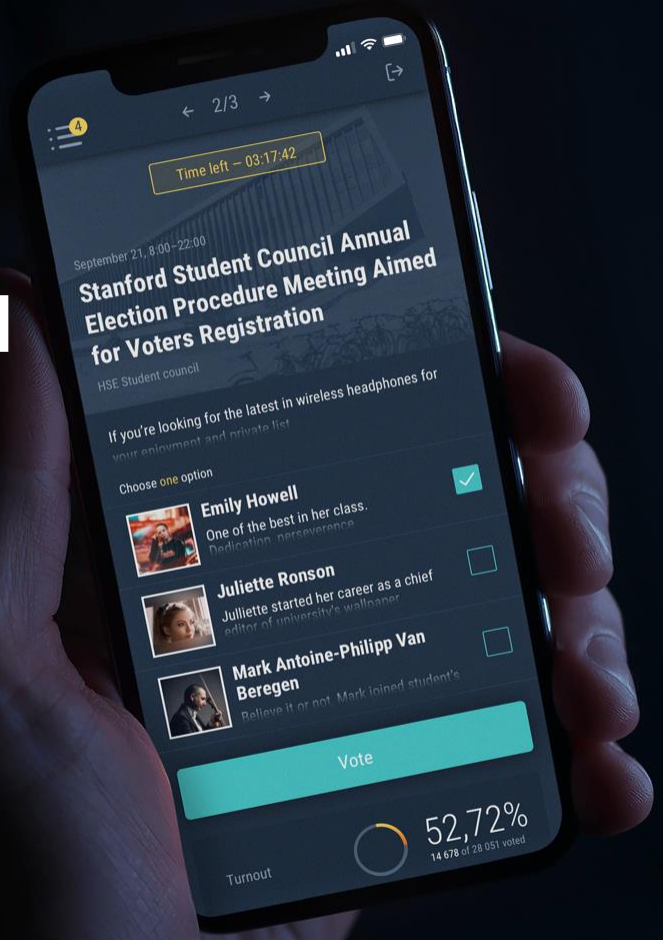
«Вброс» фальшивых голосов

Подделка результатов голосования

Запуск состоялся в 2017 году

Евгений Касперский,
основатель и директор «Лаборатории Касперского»

С помощью Polys любая организация может быстро проголосовать и принять решение по любому вопросу. Мы вложили в продукт всю нашу экспертизу, чтобы сделать его максимально надёжным и безопасным.



Мы собрали **самые современные** технологии

Блокчейн для записи хранения голосов обеспечивает прозрачность и защиту от манипуляций.

Современный интерфейс делает цифровое голосование таким же простым, как опускание бюллетеня в ящик.

Наша **экспертиза в области кибербезопасности** защищает голоса от взлома.

Задача

Организатор может изменить голос после подачи.

Решение

Блокчейн не позволяет менять данные после записи.

Задача

Организатор может создавать поддельные аккаунты избирателей.

Решение

Аккаунты избирателей фиксируются до начала голосования.

Задача

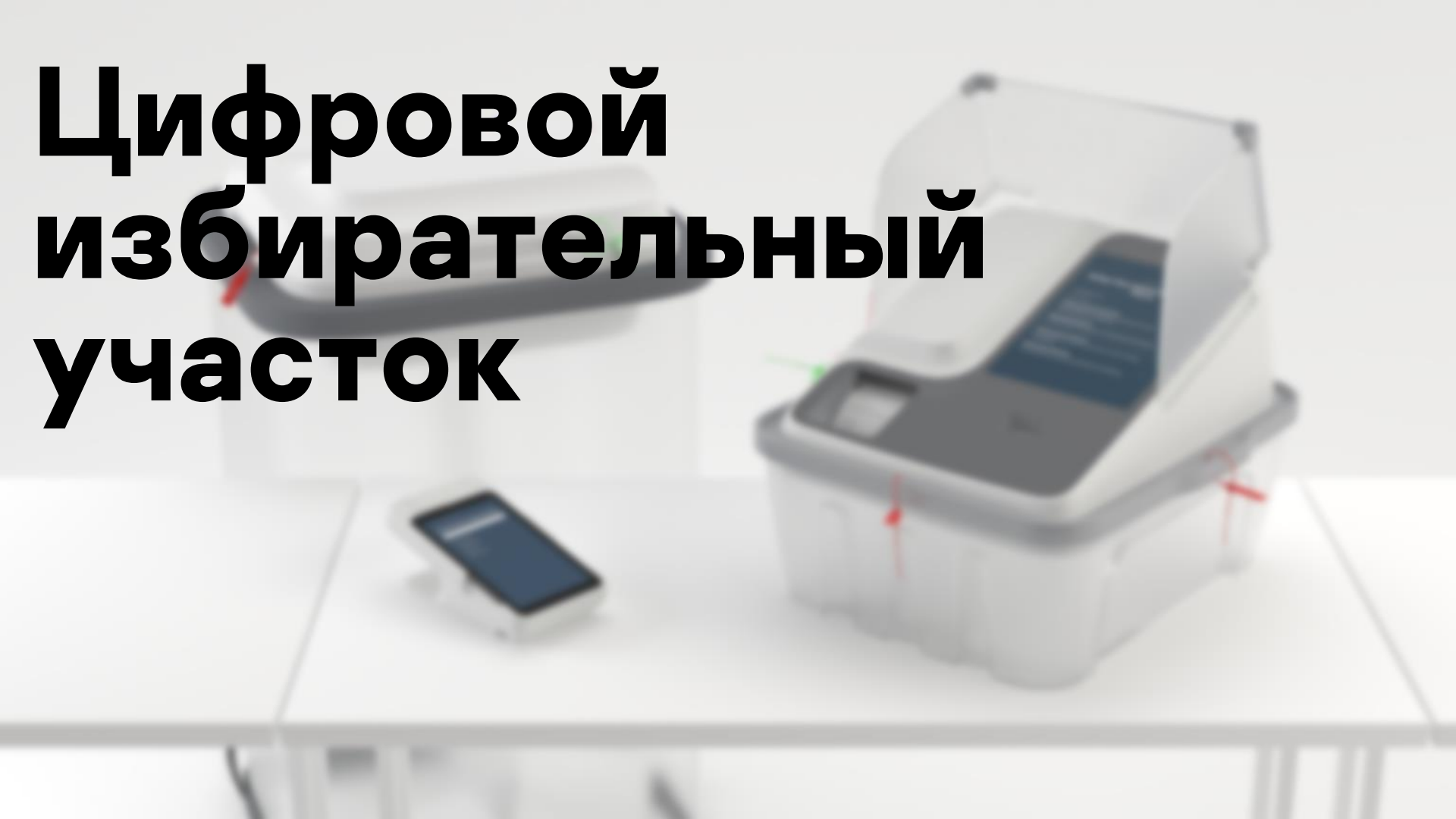
Организатор может подделать результаты голосования.

Решение

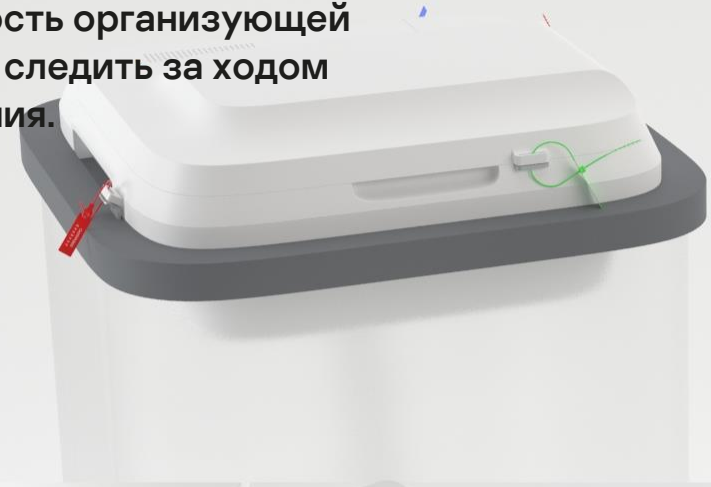
Бизнес-логику подсчета результатов нельзя изменить

Мы понимаем, что онлайн-голосования недостаточно, поэтому соединили дистанционное голосование и голосование на участке общей платформой.

Цифровой избирательный участок



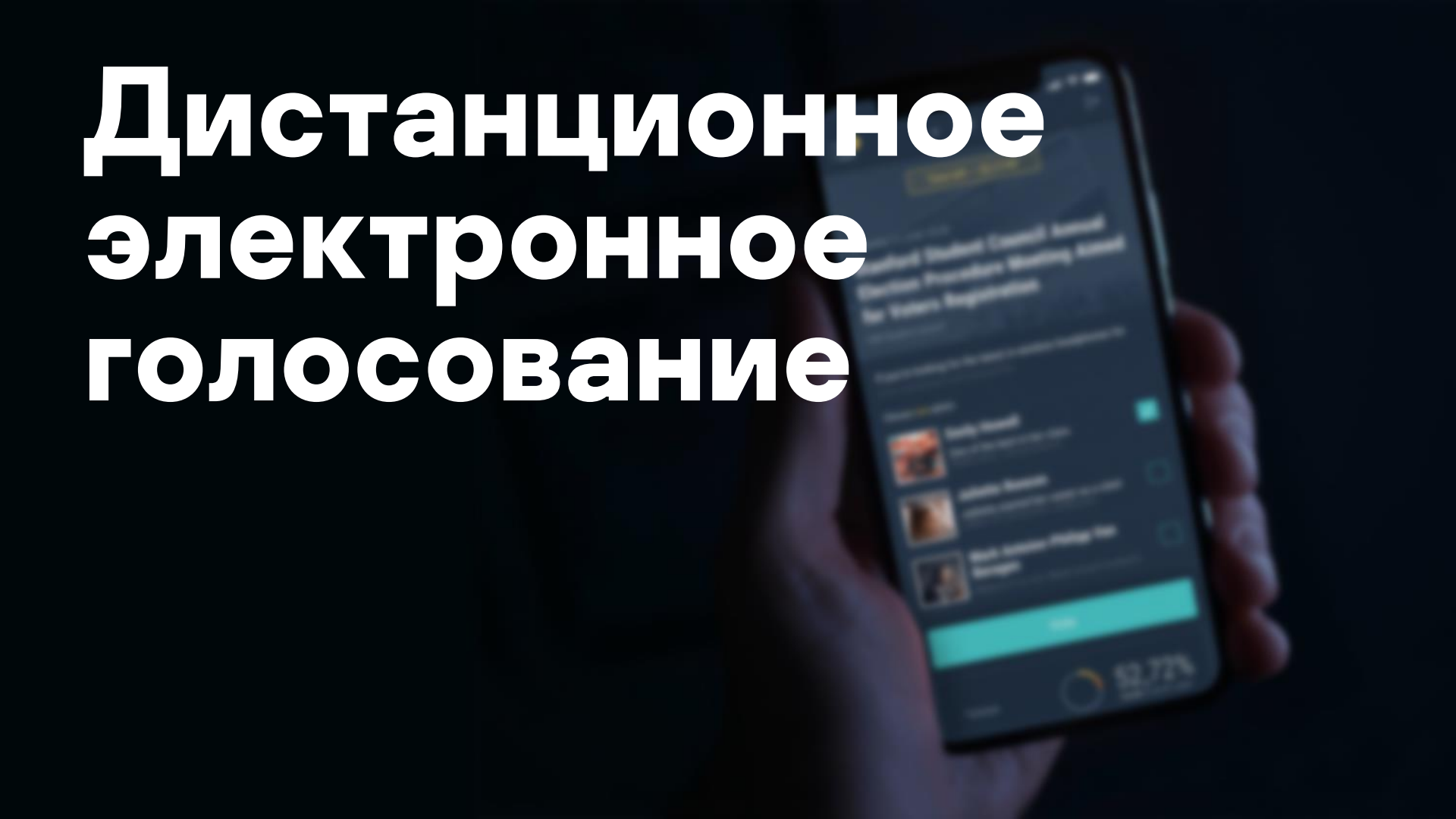
Принтер для печати поданных бюллетеней — дает возможность организующей комиссии следить за ходом голосования.



Активатор токена для голосования — активирует бюллетени для выборов и дает возможность проверить поданный голос.

Терминал для голосования — позволяет проголосовать на участке и получить бумажное подтверждение.

Дистанционное электронное голосование



Область применения

Досрочное голосование
Позволяет снизить нагрузку на избирательные участки до дня голосования.

День голосования
Предоставляет больше инструментов голосования для избирателей.

Экстерриториальное голосование
Даёт возможность голосовать избирателям, которые не имеют доступа к избирательным участкам.

Почему Polys?

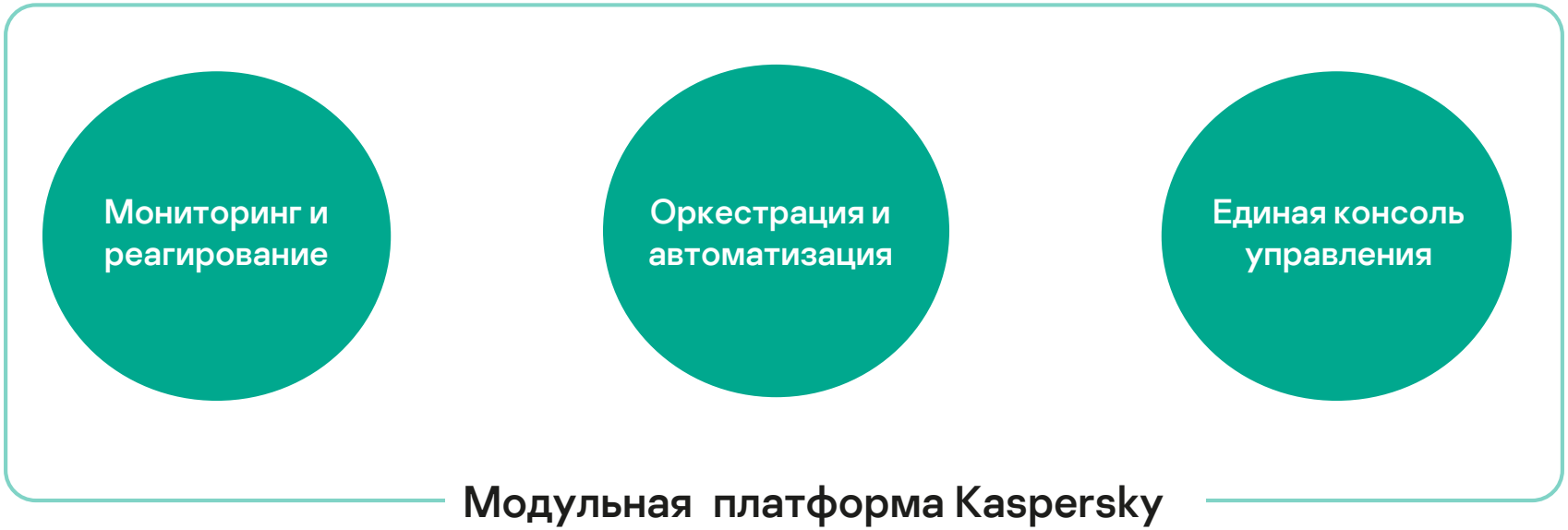
Решение находится в реестре отечественного ПО

Лаборатория Касперского имеет ряд успешных пилотов и внедрений Polys

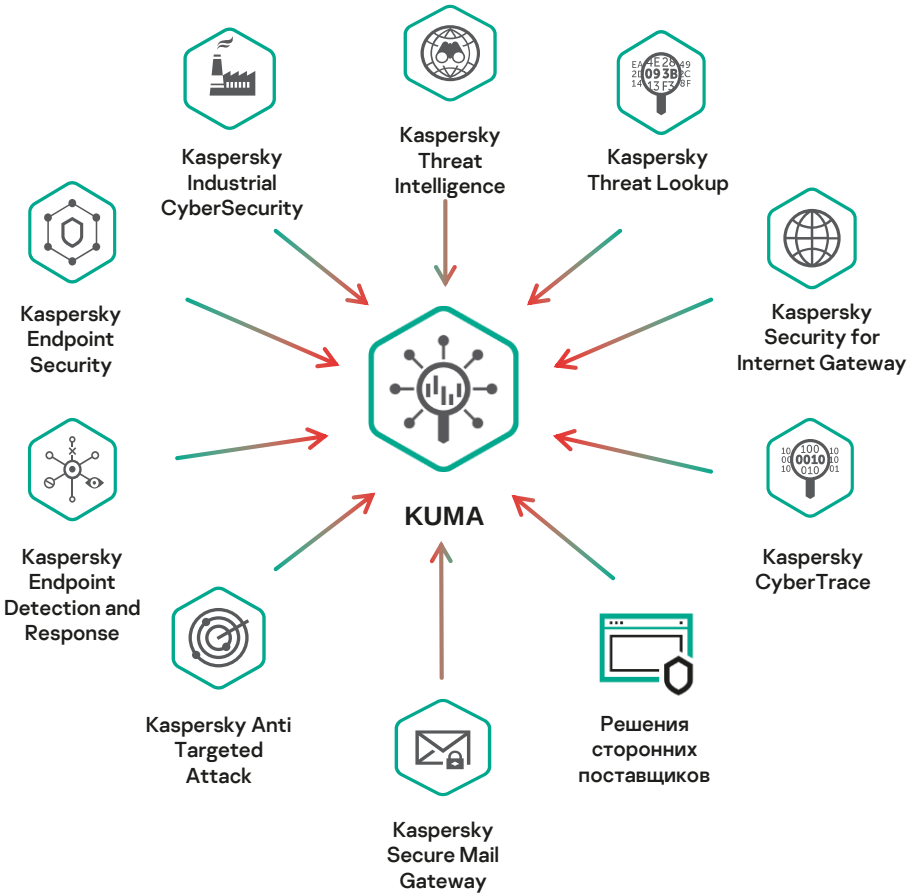
Лаборатория Касперского — лидер в области защиты информации

Kaspersky Unified Monitoring and Analysis Platform

Основные задачи управления событиями ИБ


Мониторинг и реагирование
Оркестрация и автоматизация
Единая консоль управления
Модульная платформа Kaspersky

Kaspersky Unified Monitoring and Analysis Platform



Единая консоль **мониторинга и реагирования** на инциденты ИБ

Ключевые преимущества

Производительность

370k+ EPS на одну ноду (коррелятор, ~ 100 правил)

Гибкая архитектура

Современная микросервисная архитектура

Низкие системные требования

Интеграции «из коробки»

С решениями «Лаборатории Касперского» и сторонних поставщиков

~40k EPS

Correlator + Collector + Core

Коллектор:

- CPU – 8 vCPU
- RAM – 4 ГБ;
- Storage – 100 ГБ

Коррелятор:

- CPU – 8vCPU;
- RAM – 16 ГБ;
- Storage – 100 ГБ

Ядро:

- CPU – 4 vCPU
- RAM – 8 ГБ;
- Storage – 50 ГБ

Хранилище событий (Elastic)

CPU– 24 vCPU

RAM – 48 ГБ;

Storage– 500* ГБ

*объем хранилища зависит от длительности хранения событий

KUMA Scope 2020

- Единая модель данных
- GUI
- Поддержка кастомизации парсеров
- Поддержка 3rd party источников «из коробки»
- Поддержка сохранение «сырых» событий
- Поддержка Active List
- Ретроспективный анализ (ретроскан)
- Поддержка режимов отказоустойчивости и балансировки
- Настраиваемые дашборды и отчеты
- RESTful API
- Role-based Access Control
- Обогащение событий ИБ через LDAP, DNS, Kaspersky CyberTrace, Kaspersky ThreatLookup
- Автоматическая инвентаризация активов с Kaspersky Endpoint Security
- Функции автоматизированного реагирования с Kaspersky EDR

KUMA Roadmap* 2021

(* - основные направления развития)

- Локализация UI
- Сертификация по требованиям ФСТЭК (ТУ, НДВ4)
- Реестр отечественного ПО
- Интеграция с НКЦКИ и соответствия требованиям ГосСОПКА
- Поддержка функций регистрации и учета инцидентов (case management)
- Поддержка иерархической модели развертывания SIEM (Головные и подчиненные ноды)
- Развитие функционала управления активами (asset management)
- Развитие функционала обогащения событий
- Развитие функций автоматизированного реагирования
- Расширение списка интеграций с решениями «Лаборатории Касперского»
- Расширение списка поддерживаемых «из коробки» источников данных
- Авто-приоритизация инцидентов с использованием методов Machine Learning и информации Threat Intelligence (ML- & TI-assisted auto triage)
- Multitenancy

Пилот – это просто?

Спасибо!

Александр Комиссаров

инженер предпродажной поддержки
Alexander.Komissarov@kaspersky.com
+7 (969) 730 89 30
linkedin.com/in/alexander-komissarov

kaspersky