# “Защита КИИ и реализация функций ГосСОПКА: типовые сценарии от Лаборатории Касперского”

Александр Тищенко
инженер предпродажной поддержки в ЮФО и СКФО

KASPERSKY lab

# ФЗ №187 «О безопасности критической информационной…

РОССИЙСКАЯ ФЕДЕРАЦИЯ

**ФЕДЕРАЛЬНЫЙ ЗАКОН**

**О безопасности критической информ**
**инфраструктуры Российской Фе**

Принят Государственной Думой

Одобрен Советом Федерации 19

ВСТУПИЛ В СИЛУ 01.01.2018

Статья 1. **Сфера действия настоящего Федерального закона**

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также – критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Статья 2. **Основные понятия, используемые в настоящем Федеральном законе**

Для целей настоящего Федерального закона используются следующие основные понятия:

2 100039 04559 6

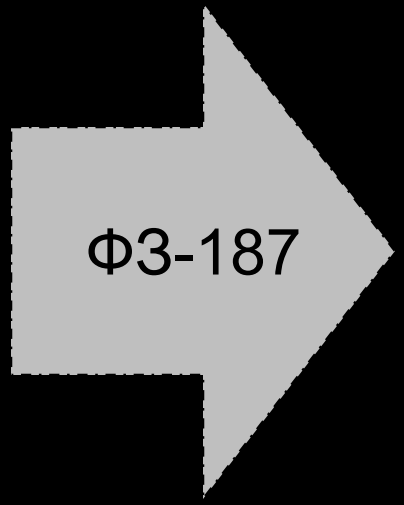


KASPERSKY lab

# ФЗ-187: драйвер перехода от защиты по остаточному принципу к построению комплексной стратегии

## От продуктов защиты

• средства обнаружения и предотвращения вторжений, в том числе обнаружения целевых атак;
• специализированные решения по защите информации для индустриальных сетей, финансового сектора;
• средства выявления и устранения DDoS-атак;
• средства сбора, анализа и корреляции событий;
• средства анализа защищенности;
• средства антивирусной защиты;
• средства межсетевого экранирования;
• средства криптографической защиты информации и защищенного обмена данными.

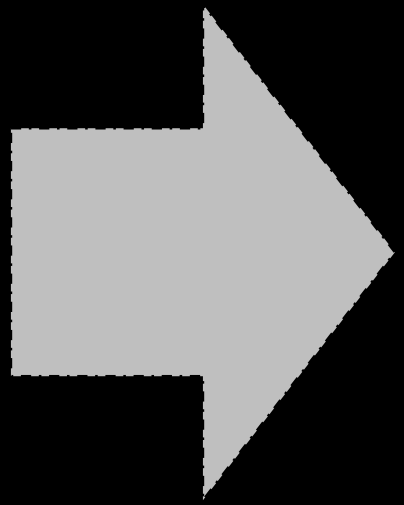



## К построению зрелых процессов

• инвентаризация информационных ресурсов;
• выявление уязвимостей ИТ ресурсов;
• анализ угроз информационной безопасности;
• повышение квалификации персонала;
• прием сообщений о возможных инцидентах от персонала и пользователей ИТ ресурсов;
• обеспечение процесса обнаружения компьютерных атак;
• анализ данных о событиях безопасности;
• регистрация инцидентов;
• реагирование на инциденты и ликвидация их последствий;
• установление причин инцидентов;
• анализ результатов устранения последствий инцидентов.

# ГОССОПКА

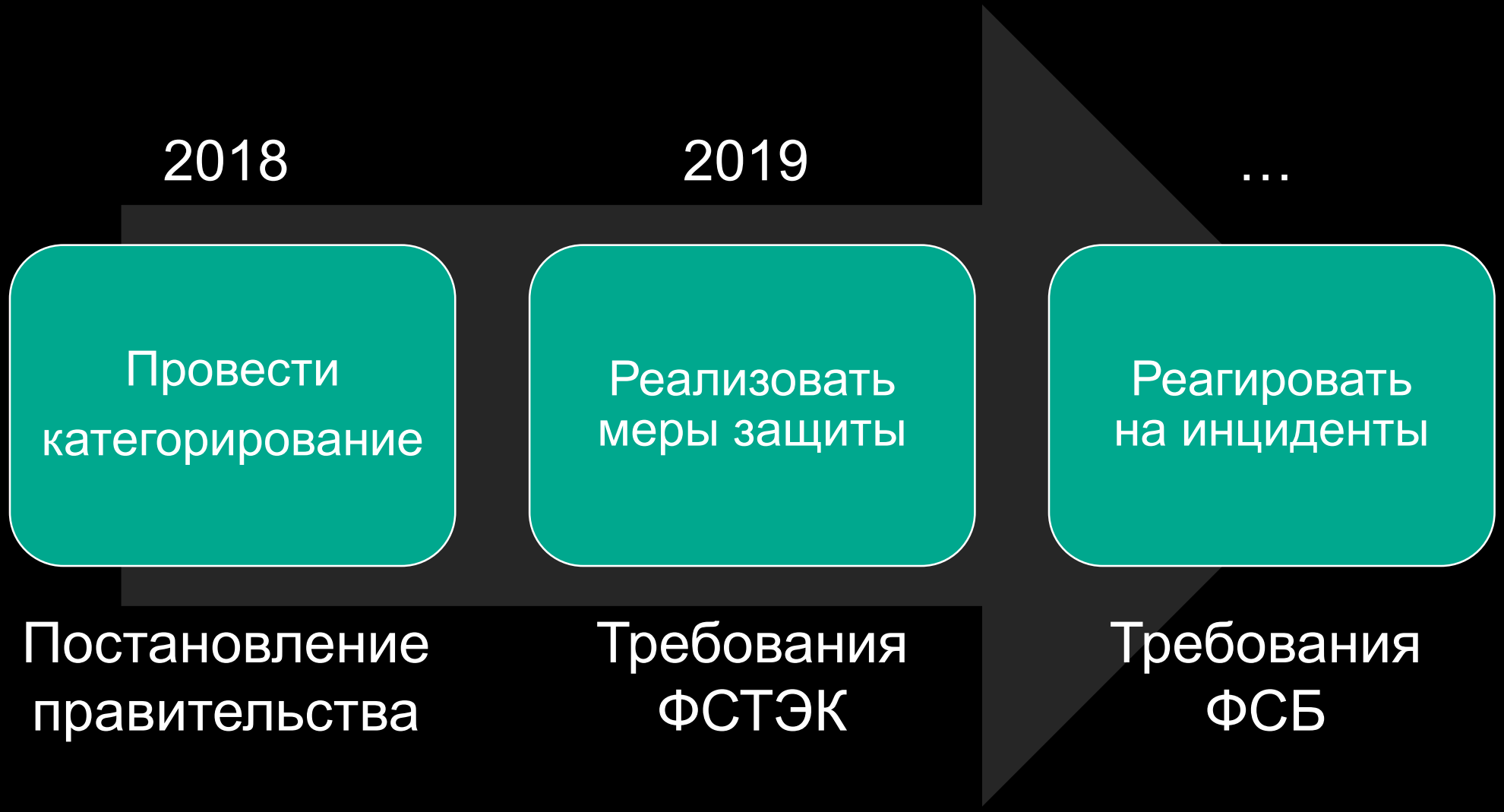
Продукты и сервисы «Лаборатории Касперского» отвечают большинству требований к функциям центров ГосСОПКА. Кроме технического соответствия, они обеспечивают защиту нового поколения, которая базируется на сочетании машинного обучения, передовых технологий и экспертного опыта в области изучения и анализа угроз, накопленного за более чем 20 лет работы. Подробнее о каждом продукте и сервисе и его возможностях применительно к центрам ГосСОПКА вы можете узнать у наших специалистов.



- Инвентаризация информационных ресурсов
- Выявление уязвимостей
- Анализ угроз ИБ
- Повышение квалификации персонала
- Обеспечение процесса обнаружения компьютерных атак
- Анализ данных о событиях безопасности
- Регистрация инцидентов
- Реагирование на инциденты и ликвидация их последствий
- Установление причин инцидентов
- Анализ результатов

https://gossopka.kaspersky.ru/

# Что нужно делать?



# Адаптивная стратегия корпоративной ИБ

## ПРОГНОЗИРОВАНИЕ

- Тесты на проникновение
- Оценка защищенности приложений
- Сервис Targeted Attack Discovery
- Kaspersky Threat Intelligence Portal
- Подписка на APT отчеты

## ПРЕДОТВРАЩЕНИЕ

- Тренинги по ИБ
- Специализированные решения защиты
  - Защита рабочих мест
  - Защита дата-центров
  - Безопасность встроенных систем
  - …
- Повышение осведомленности
- Индустриальная безопасность

## РЕАГИРОВАНИЕ

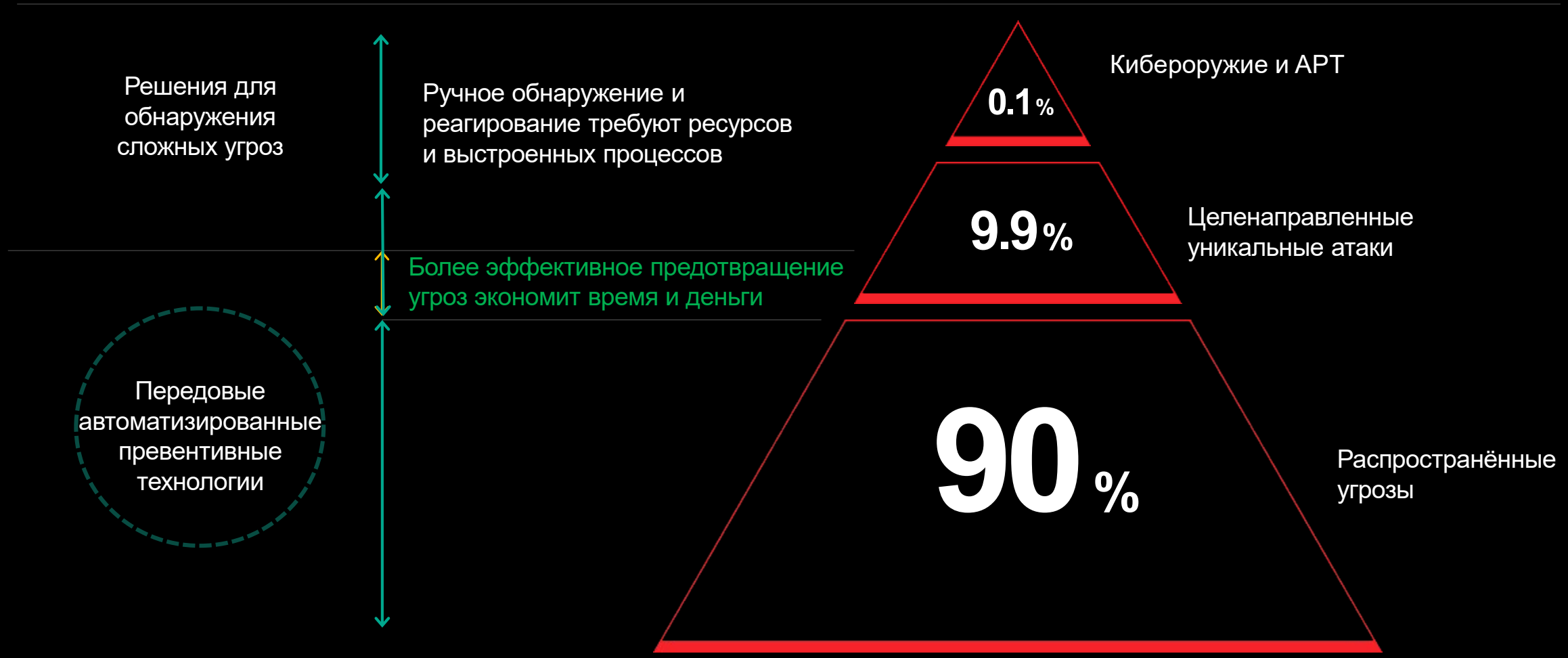
- Премиальная поддержка – Maintenance Security Agreement
- Сервис реагирования на инциденты
- Цифровая криминалистика
- Анализ ВПО
- Endpoint Detection & **Response**

## ОБНАРУЖЕНИЕ

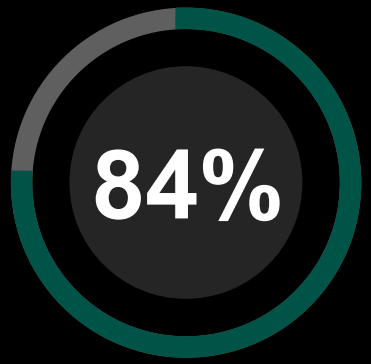
- Кастомизированные отчеты
- Threat data feeds
- Kaspersky Threat Deception
- Kaspersky Managed Protection
- Kaspersky Anti Targeted Attack (KATA)
- Endpoint **Detection** & Response

# Чем больше угроз будет автоматически заблокировано, тем дешевле

Роль решений с максимальной эффективностью блокирования угроз



# А нужна ли в 2019 году защита рабочих мест и серверов?




## Успешных атак на конечные точки затрагивали более 1 устройства

Несанкционированный доступ даже к одному устройству может нанести огромный вред для организации

Рабочие места – первичная цель любой кибератаки

- Уязвимы к большому числу атак
- Их много и они все разные
- Есть AV ну и бог с ним
- Хранят идентификационные данные
- Начальная точка развития целевой атаки

**Endpoint Protection and Response: A SANS Survey, 2018*

# Kaspersky Lab ICS CERT зафиксировал атаку

В 2018 г. которой подверглись не менее 400 промышленных компаний России, относящихся к следующим индустриям:

- производство
- нефть и газ
- металлургия
- инжиниринг
- энергетика
- добыча полезных ископаемых
- логистика

СУБЪЕКТЫ КИИ

08 August 2018

CYBER KILL CHAIN



TeamViewer

KASPERSKY lab

AO Kaspersky Lab [RU] https://securelist.ru/attacks-on-indust

SECURELIST УГРОЗЫ КАТЕГОРИИ

ИНДУСТРИАЛЬНЫЕ УГРОЗЫ

# Атаки на промышл предприятия с исп и TeamViewer

Вячеслав Копейцев, Мария Гарнаева, Кирилл Кругл

СОДЕРЖАНИЕ

## Основные факты

Kaspersky Lab ICS CERT зафиксировал очередную волну ра нацеленных преимущественно на компании и организаци промышленным производством.

Фишинговые письма замаскированы под легитимные ком промышленным компаниям на территории РФ. Содержан организации и учитывает специфику работы сотрудника -

Согласно собранным данным, эта серия атак началась в н этом первые подобные атаки были зафиксированы ещё в

редоносная программа, используемая в данных атаках, у

Kaspersky
Threat Intelligence Portal

Home | Reporting | Threat Lookup | WHOIS Tracking | Cloud Sandbox | Data Feeds | Licensing

You are using a demo version of the service. Purchase commercial licenses: Licensing

Use the hash symbol (#) to add tags to the query

Search

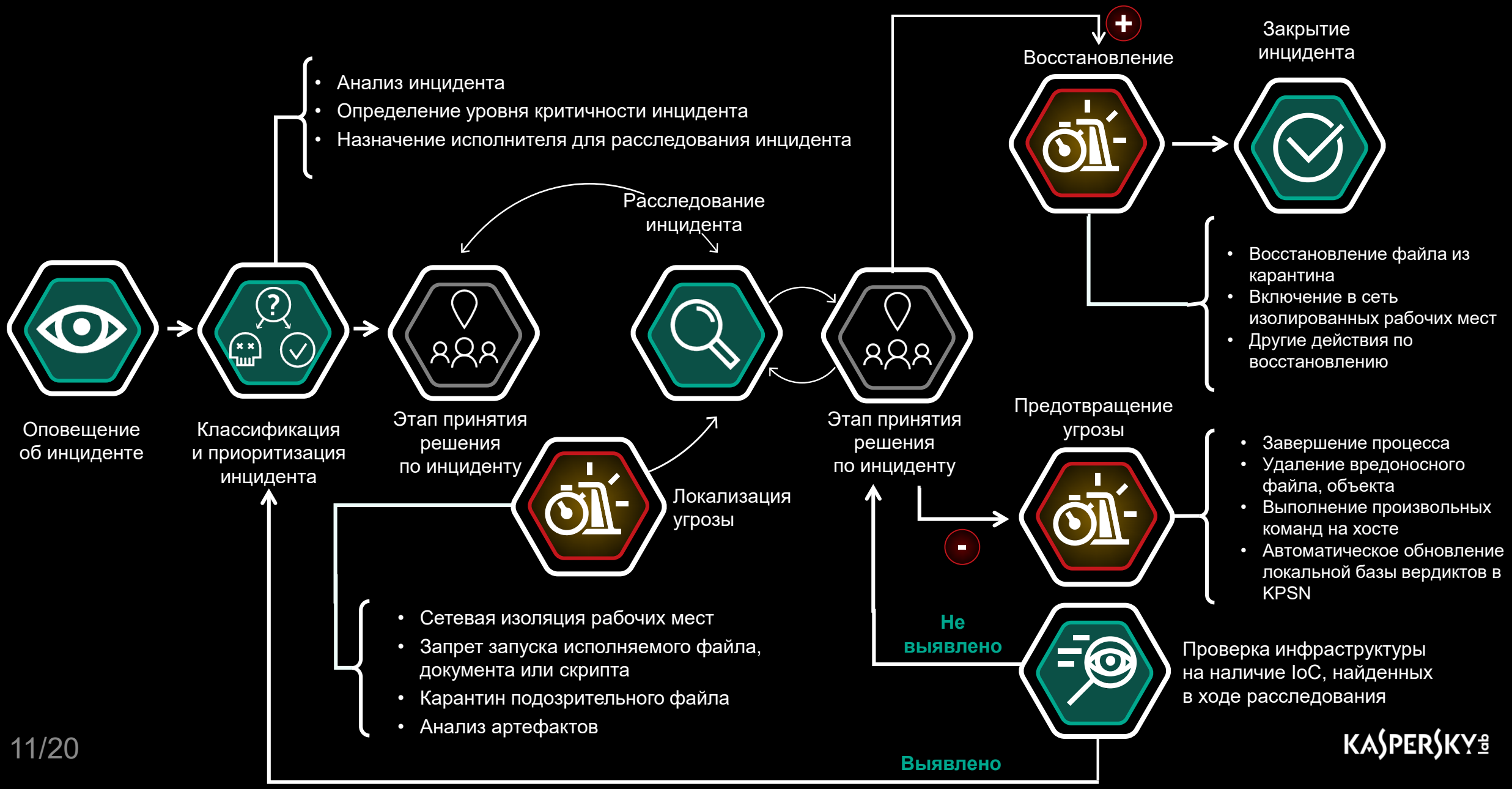
APT (demo) Financial (demo) Industry (0) Geo (0) Actor (0) Show period Month Year All Custom

## APT Reports

Master YARA (APT) Master IOC (APT) Master YARA (Financial) Master IOC (Financial) (available only for commercial licenses)

| | | |
|---|---|---|
| Apr 26, 2017 | Sofacy Using Two Zero Days in Recent Targeted Attacks - early warning<br>Download YARA Rule \| IOC \| Report (En) \| Executive summary (En) | Europe, Sofacy |
| Apr 20, 2017 | ShadowBrokers Lost in translation leak - SWIFT attacks analysis<br>Download IOC \| Report (En) \| Executive summary (En) | Belgium, Equation group, Financial institutions |
| Mar 31, 2017 | Monthly APT activity report - March 2017<br>Download Report (En) | |
| Mar 09, 2017 | APT10 Spearphishes Japanese Policy Experts late 2016 to early 2017<br>Download YARA Rule \| IOC \| Report (En) \| Executive summary (En) | Japan, APT10 |
| Feb 22, 2017 | Ismdoor - possible Shamoon attack vector found in Saudi Arabia<br>Download YARA Rule \| IOC \| Report (En) \| Executive summary (En) | Iraq, Energy, Jordan, Qatar |
| Feb 03, 2017 | New Wave of BlueNoroff Attacks against Polish banks<br>Download YARA Rule \| IOC \| Report (En) \| Executive summary (En) | Poland, BlueNoroff, Finan |
| Aug 23, 2018 | Report is available only for commercial license | |
| Aug 21, 2018 | Report is available only for commercial license | Bahrain, Diplomatic, Mauritius, Government, Pakistan, IT con |

# Типовой пример действий по централизованному реагированию



# Поэтапная стратегия развития кибербезопасности

Единая долгосрочная стратегия развития кибербезопасности с учетом уровня и темпов роста компетенций в области ИБ

Блокирование максимального количества угроз в автоматическом режиме

Автоматизация передовых средств обнаружения и защиты

Развитие передовой экспертизы для комплексной защиты

## Этап 1

Оценить и максимально усилить существующие превентивные технологии

Минимизировать необходимость ручного анализа

## Этап 2

Выстроить максимально эффективную и удобную защиту от передовых угроз

Автоматизировать ручные операциии службы ИБ для повышения эффективности

## Этап 3

Внедрение концепции SOC, постоянного мониторинга и максимальной осведомленности о происходящем в сети

и настр ии
ласности

# Сотрудники – самое слабое звено

**52%** считают, что наибольшую угрозу системе корпоративной безопасности представляют сами сотрудники*.

**60%** сотрудников хранят на своих рабочих устройствах конфиденциальные данные (финансовая информация, базы e-mail и т.д.)**


**30%** сотрудников признались, что делились логином и паролем от рабочего компа с коллегами**.

**23%** организаций не создают для своих сотрудников правила безопасности относительно хранения рабочих данных**

KASPERSKY lab

# Чем мы можем помочь?

**Непрозрачная инфраструктура**
Индустриальные сети строятся и поддерживаются фрагментарно в разное время, нет единой точки мониторинга

**Локальные практики базовой ИБ**
На разных установках – разные средства и политики ИБ, нет централизации даже для самых простых мер (АВ, контроль устройств..)

**Неосведомленность персонала**
Нехватка специалистов в ИБ АСУ ТП. Неосведомленность о рисках среди инженерного состава

Анализ Защищенности

**Оценка текущей защищенности и конкретные рецепты ее повышения**

Анализ трафика

**Инвентаризация тех сети и выявление вторжений**

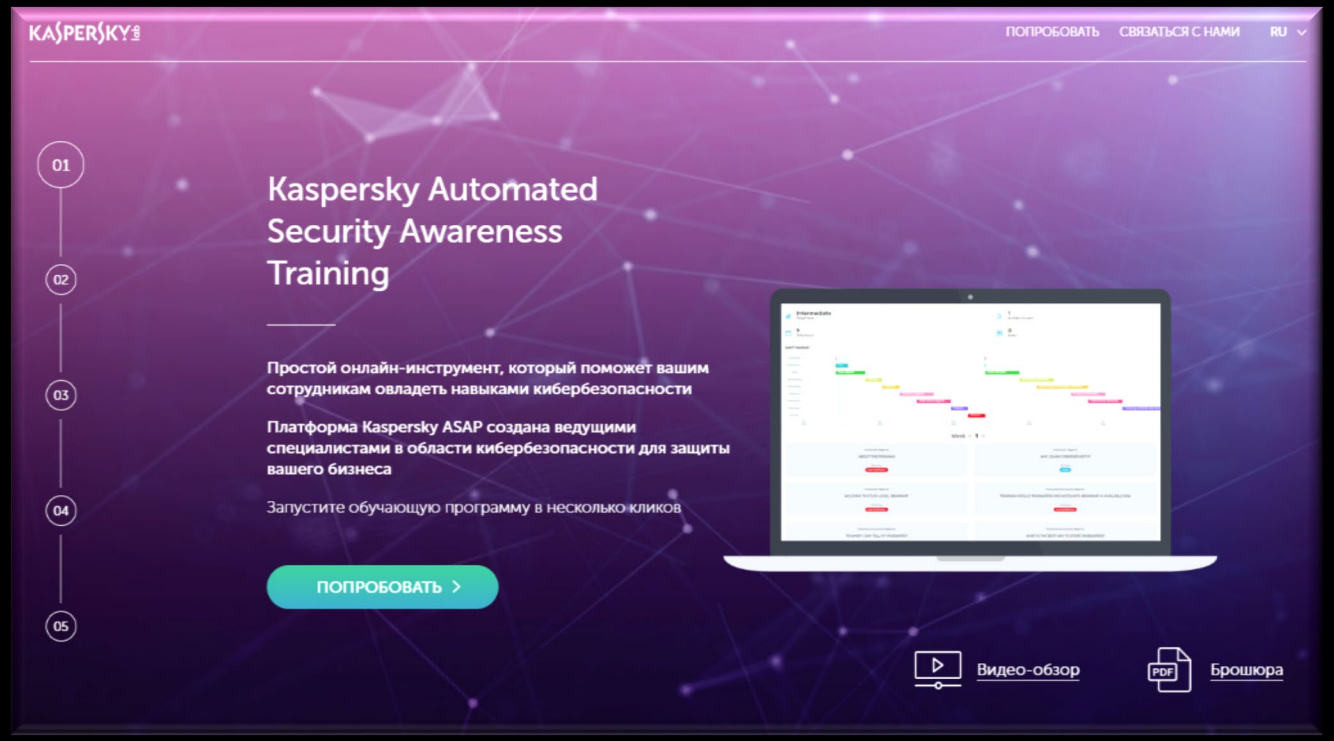
Защита Endpoint

**Централизованные базовые средства защиты для всей инфраструктуры**

Обучающие программы

**Тренинги (Профессиональные и для широкого круга)**

# Новая платформа обучения навыкам – Kaspersky ASAP




- **«Запрограммированная» эффективность обучения**

  Новый навык каждый день + интервальная тренировка + постоянное закрепление + измерение прогресса в числе навыков

- **Почти нулевые трудозатраты на управление**

  Полная автоматизация – настройка и запуск обучения занимает несколько минут. Бесплатный триал. Покупка от 5 лицензий

- **Онлайн-платформа**

  Автоматический план обучения, оценка знаний

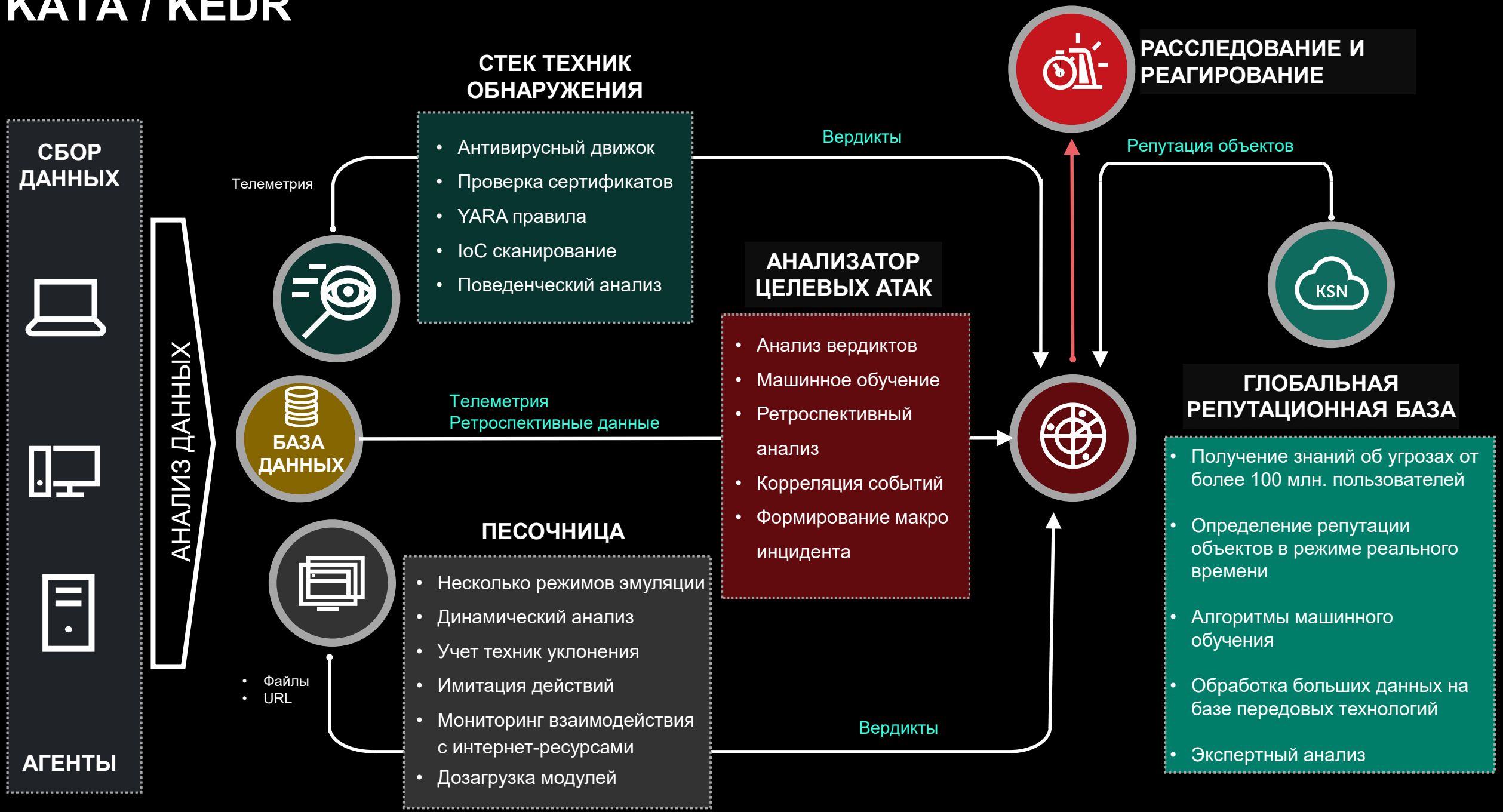
Получить бесплатный триал:

www.k-asap.ru

Видео-обзор:

youtu.be/7XLYLauDRMY

# KATA / KEDR

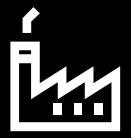

СБОР ДАННЫХ
АГЕНТЫ
АНАЛИЗ ДАННЫХ
Телеметрия
СТЕК ТЕХНИК ОБНАРУЖЕНИЯ
• Антивирусный движок
• Проверка сертификатов
• YARA правила
• IoC сканирование
• Поведенческий анализ
Вердикты
РАССЛЕДОВАНИЕ И РЕАГИРОВАНИЕ
Репутация объектов
KSN
БАЗА ДАННЫХ
Телеметрия
Ретроспективные данные
АНАЛИЗАТОР ЦЕЛЕВЫХ АТАК
• Анализ вердиктов
• Машинное обучение
• Ретроспективный анализ
• Корреляция событий
• Формирование макро инцидента
ГЛОБАЛЬНАЯ РЕПУТАЦИОННАЯ БАЗА
• Получение знаний об угрозах от более 100 млн. пользователей
• Определение репутации объектов в режиме реального времени
• Алгоритмы машинного обучения
• Обработка больших данных на базе передовых технологий
• Экспертный анализ
ПЕСОЧНИЦА
• Несколько режимов эмуляции
• Динамический анализ
• Учет техник уклонения
• Имитация действий
• Мониторинг взаимодействия с интернет-ресурсами
• Дозагрузка модулей
• Файлы
• URL
Вердикты

# Помощь в соответствии требованиям/рекомендациям регуляторов

**1**

**Обеспечиваем передовую защиту КИИ и инфраструктуры фин.институтов рабочих станций и серверов, сокращая риски ИБ**

## Компании с КИИ



**Критическая информационная инфраструктура**

- 187 ФЗ
- ГосСОПКА
- Российское ПО
- Сертификаты ФСТЭК, ФСБ
- Изоляция

## Компании из финансового сектора

**Финансовые институты**

- ФинЦерт
- PCI DSS
- N 152-ФЗ, GDPR
- 187 ФЗ
- ГосСОПКА

**2**

**Помогаем следовать требованиям/ рекомендациям регулирующих органов**

- Сертификаты ФСТЭК, ФСБ
- Реестр российского ПО
- Полная изоляция от облака (KPSN)
- Нацеленность на ГосСОПКА, защиту КИИ, следование рекомендациям ФинЦерт

# Защита структур любого масштаба

Решения «Лаборатории Касперского» защищают крупные IT-инфраструктуры от актуальных киберугроз.

Контроль и защита рабочих мест

Защита виртуальных и облачных сред

Безопасность мобильных устройств

Защита от целевых атак

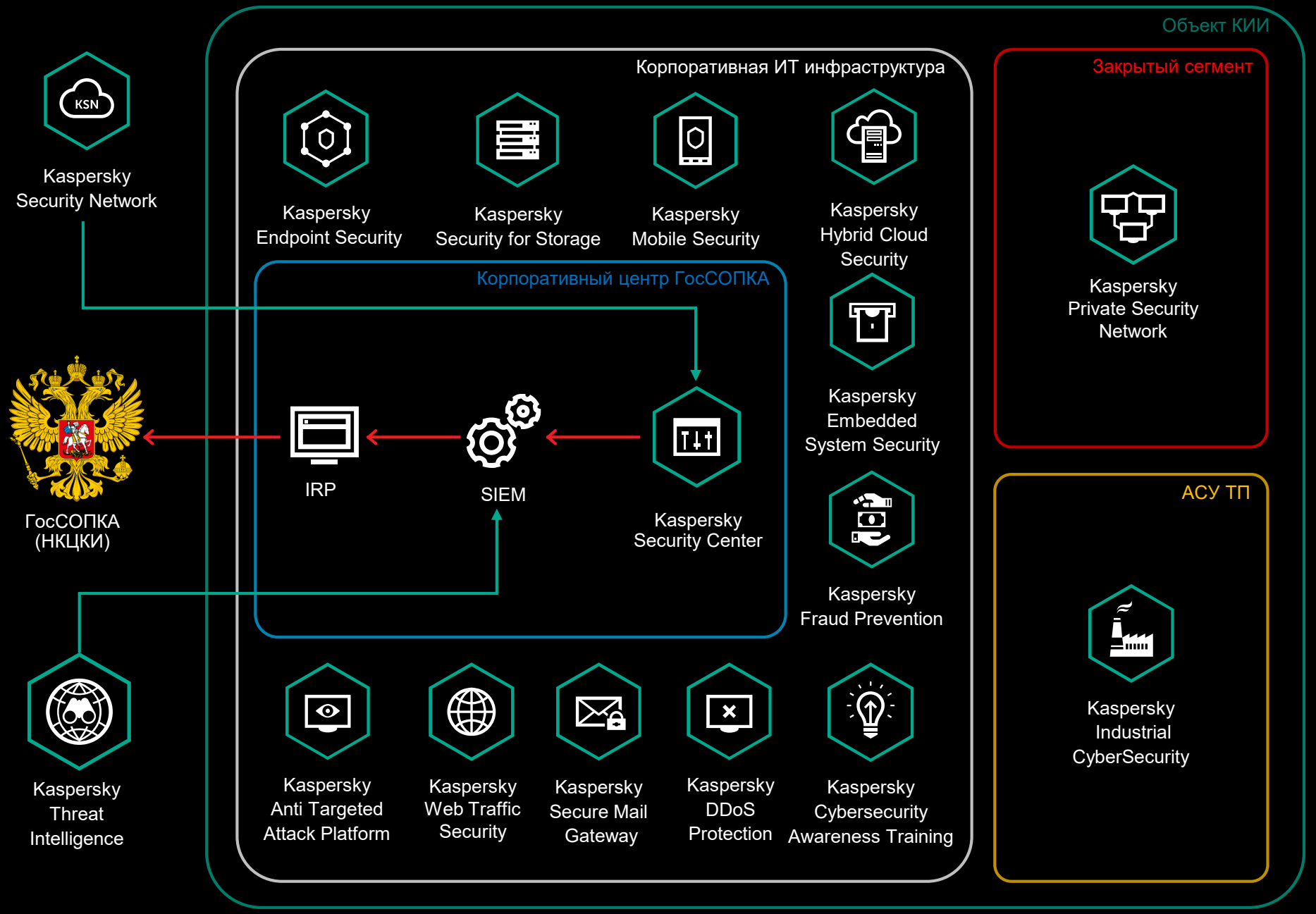
Защита от DDoS-атак

Экспертные сервисы

Защита центров обработки данных

Защита мобильного и онлайн-банкинга

Защита критических инфраструктур


Объект КИИ
Корпоративная ИТ инфраструктура
Закрытый сегмент
АСУ ТП
Корпоративный центр ГосСОПКА
KSN
Kaspersky Security Network
Kaspersky Endpoint Security
Kaspersky Security for Storage
Kaspersky Mobile Security
Kaspersky Hybrid Cloud Security
Kaspersky Private Security Network
Kaspersky Embedded System Security
Kaspersky Fraud Prevention
Kaspersky Industrial CyberSecurity
ГосСОПКА (НКЦКИ)
IRP
SIEM
Kaspersky Security Center
Kaspersky Threat Intelligence
Kaspersky Anti Targeted Attack Platform
Kaspersky Web Traffic Security
Kaspersky Secure Mail Gateway
Kaspersky DDoS Protection
Kaspersky Cybersecurity Awareness Training

# Спасибо за внимание!

Александр Тищенко
инженер предпродажной поддержки в ЮФО и СКФО
alexander.tishenko@kaspersky.com

KASPERSKY lab