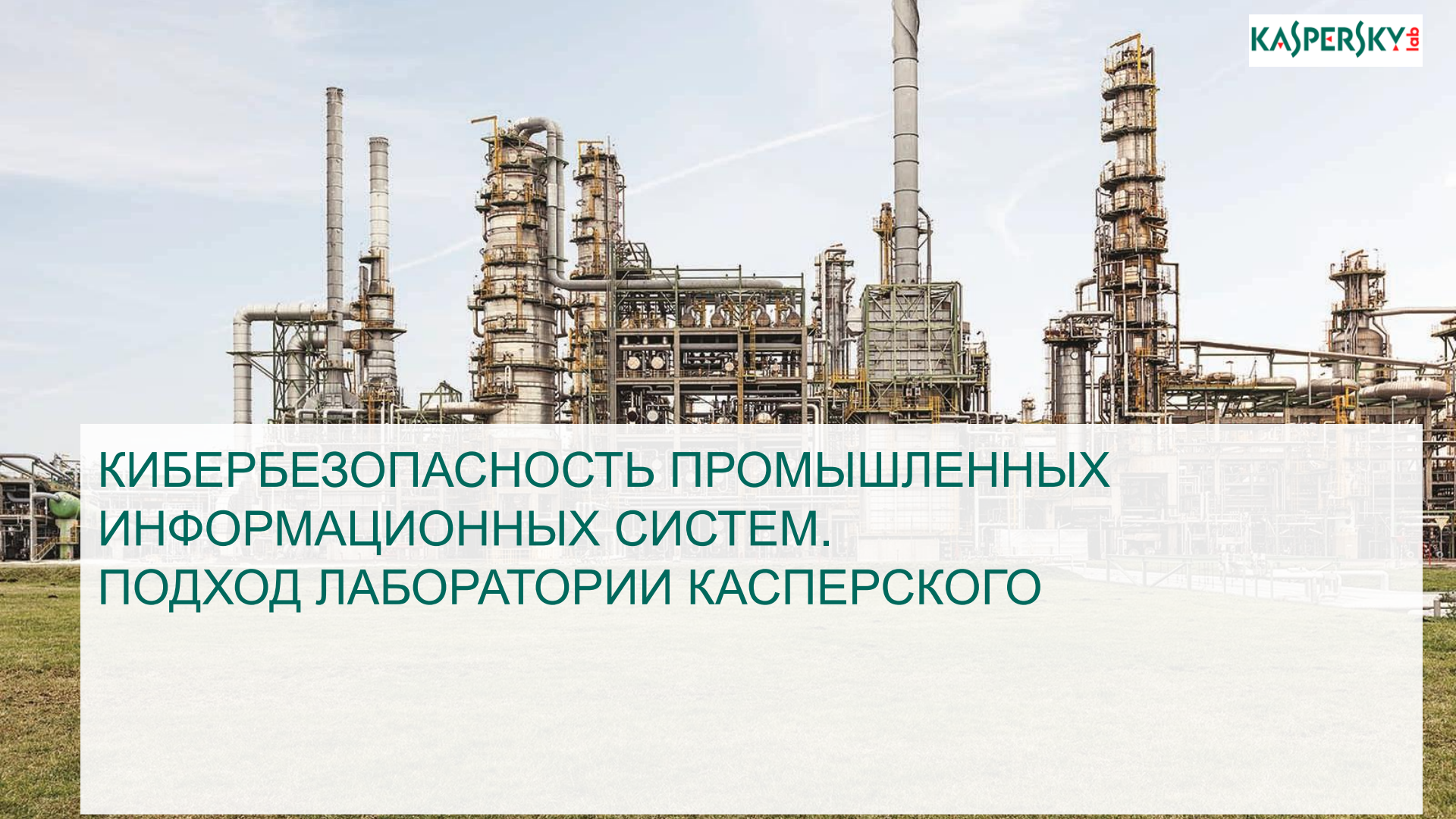


КИБЕРБЕЗОПАСНОСТЬ ПРОМЫШЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ. ПОДХОД ЛАБОРАТОРИИ КАСПЕРСКОГО

СОДЕРЖАНИЕ

Кибер-угрозы

Специфика АСУТП

Решения Лаборатории Касперского

Кибер-угрозы

Специфика АСУ ТП

Решения Лаборатории Касперского

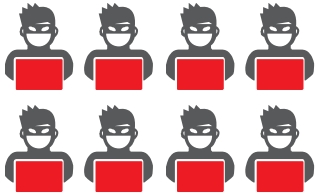
ТЕКУЩАЯ СИТУАЦИЯ ПО КИБЕРБЕЗОПАСНОСТИ АСУ ТП

по данным US ICS-CERT

Тенденция увеличения количества инцидентов в АСУ ТП:

2012

198 incidents

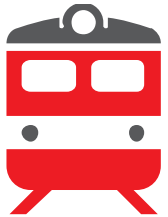


2013

~400 incidents

Большинство атак нацелено на

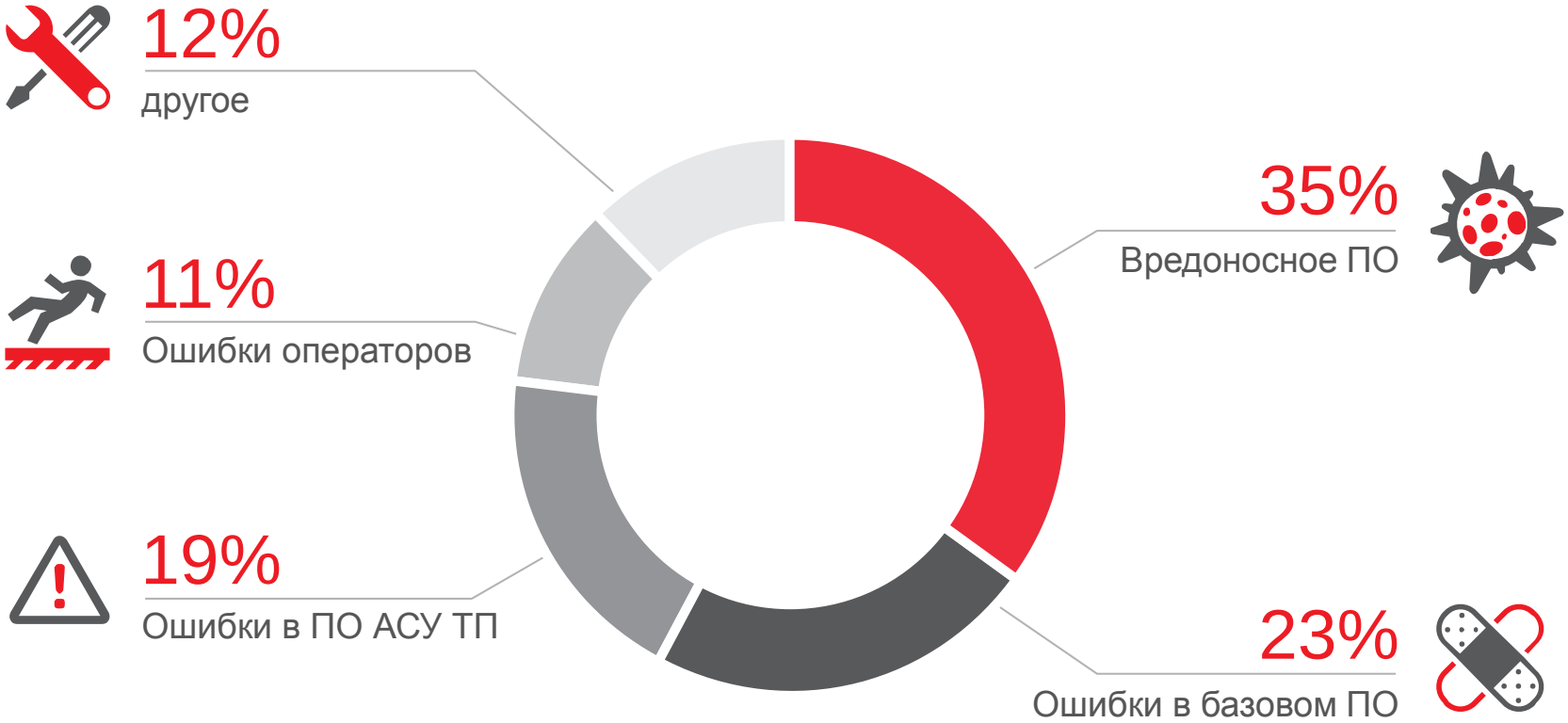
Oil & Gas, Power plants (Hydro, Nuclear)



Transportation

Основная цель — получить доступ к SCADA и PLC

ПРИЧИНЫ ИНЦИДЕНТОВ В АСУ ТП



источник: RISI Annual Summary 2013

ВРЕМЯ ПРОСТОЯ ПО ПРИЧИНЕ КИБЕР-ИНЦИДЕНТОВ

источник: RISI Annual Summary 2013

АКТУАЛЬНОСТЬ – ДОКУМЕНТИРОВАННЫЕ ИНЦИДЕНТЫ В ТЕЧЕНИИ 2014 ГОДА

	**июль 2014**. Троянец Havex из состава Energetic Bear использует среду АСУ ТП для **распостранения**. Заражает OPC-сервера и сетевые устройства, а так же зафиксированны инфицированные инсталляторы, расположенные на легитимных сайтах производителей: eWon, MB Connect Line GmbH, MESA Imaging. 2800 инцидентов по всему миру: Испания, США, Франция, Италия, Германия
	**янв. 2014**. Monju Nuclear Power Plant. Через инфицированное обновление ПО на сайте производителя был атакован компьютер в Центре управления, 42000 e-mail украдены и переправлены на сервер в Южной Корее
	**дек. 2014**. Сталелитейный завод в Германии. Федеральное управление по информационной безопасности (BSI) признало факт компьтерной атаки, в результате чего «предприятию был нанесен серьезный финансовый ущерб». Доменную печь не удалось остановить в штатном режиме

ЦЕЛЕВЫЕ АТАКИ – ИЗВЕСТНОСТЬ СПУСТЯ ГОДЫ

	Обнаружен	Активен	Период скрытности
StuxNet	2010	2005	5
NetTraveler	2013	2004	9
Icefog	2013	2010	3
Energetic Bear / Havex	2014	2010	4

То что происходит у нас сейчас мы узнаем через 3-5 лет!!!

Кибер-
угрозы

Специфика
АСУ ТП

Решения
Лаборатории
Касперского

РАЗЛИЧИЕ В ПОДХОДАХ

Корпоративная сеть

1. конфиденциальность
2. целостность
3. доступность

Офисная кибербезопасность – это защита данных

АСУ ТП

1. доступность
2. целостность
3. конфиденциальность

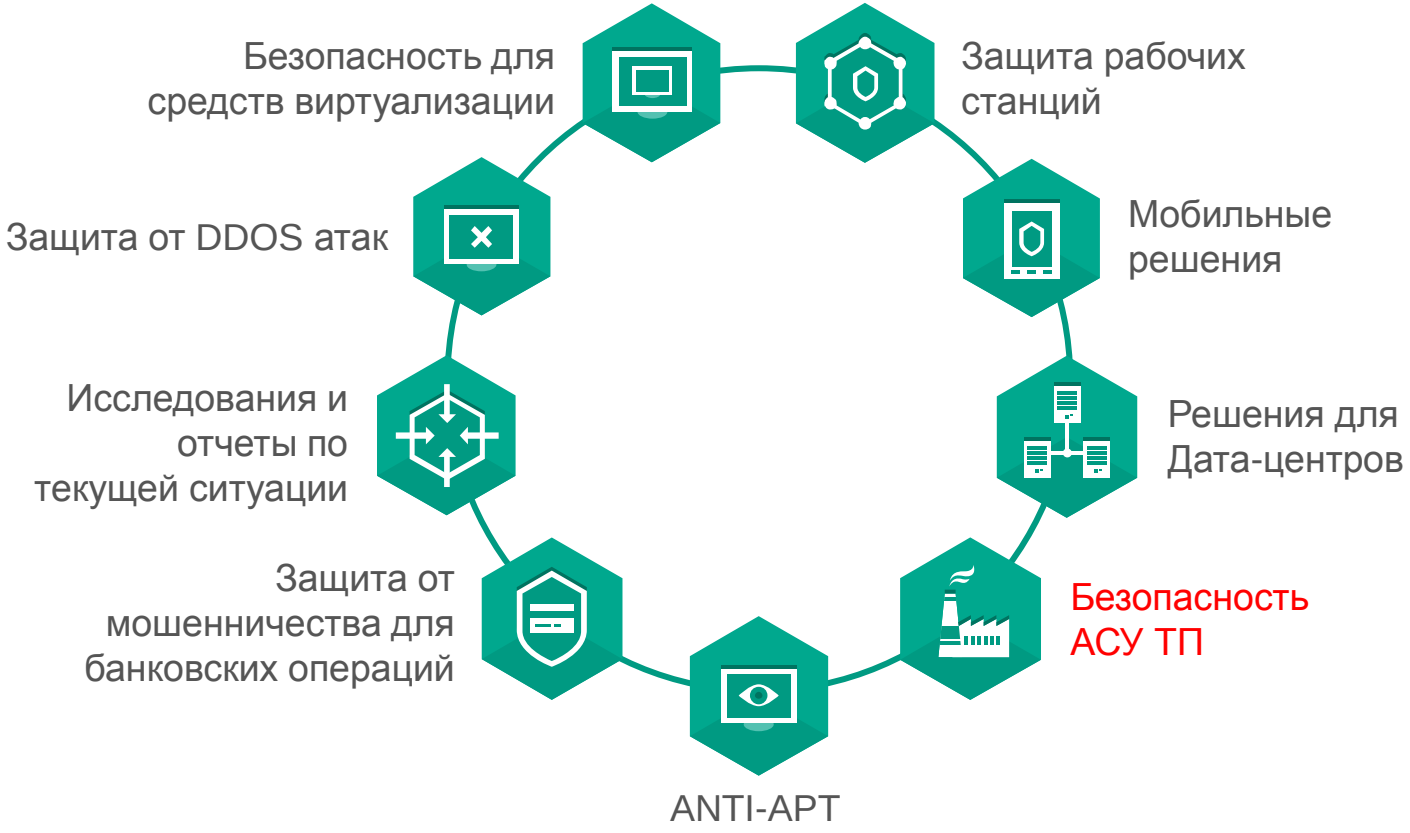
Индустриальная кибербезопасность – это защита непрерывности процесса и управления

Кибер-
угрозы

Специфика
АСУ ТП

Решения
Лаборатории
Касперского

КОМПЛЕКСНОЕ РЕШЕНИЕ ДЛЯ КОРПОРАЦИИ



КОМПЛЕКСНОЕ РЕШЕНИЕ

в соответствии с многоуровневой моделью предприятия ISA95

LEVEL 4
Business planning
and logistics

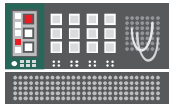
Managing end-to-end supply chain. Establishing the basic plant schedule – production, material use, delivery, and shipping.

LEVEL 3
Manufacturing
Operations management

Work flow/recipe control to produce the desired end products. Maintaining records and optimizing the production process.

LEVEL 2, 1
Batch Control.
Continuous Control.
Discrete Control.

Monitoring, supervisory control and automated control of the production process



Sensing the production process, manipulating the production process

LEVEL 0
Physical

Physical devices

Kaspersky Security for Business + Professional Services

Kaspersky Industrial Security + Professional Services

Physical security

KASPERSKY lab

КИБЕРБЕЗОПАСНОСТЬ ЭТО ПРОЦЕСС, А НЕ АКЦИЯ

ФАЗЫ ПРОЕКТА КИБЕРЗАЩИТЫ

Сбор требований	Обследование и оценка	Разработка проекта	Пилотный проект	Реализация	Поддержка и сервисы
Формирование тех. задания определение векторов угроз	обследование объекта модель угроз и анализ рисков рекомендации по гармонизации регламентной документации	выбор средств защиты и компенсационных мер Проектирование комплекса	Пилотная реализация на выбранном объекте	внедрение на объектах Обучение специалистов	24x7 регулярная поддержка, послепродажные сервисы Расследования инцидентов решение проблем

СТРУКТУРА КОМПЛЕКСНОГО ПРЕДЛОЖЕНИЯ

Технологии защиты объектов АСУ ТП: , HMI, рабочие станции, PLC, сеть, интеллектуальные устройства

Полсепродажное обслуживание и сервисы

Для регулирующих органов

Консультирование и экспертиза по разработке отраслевых стандартов и регулирующих документов

Профессиональные сервисы

- Обучение и повышение квалификации
- Раннее оповещение
- Расследование киберинцидентов
- Управляемая защита (проактивное предупреждение инцидентов)
- И другие сервисы

Для проектных организаций

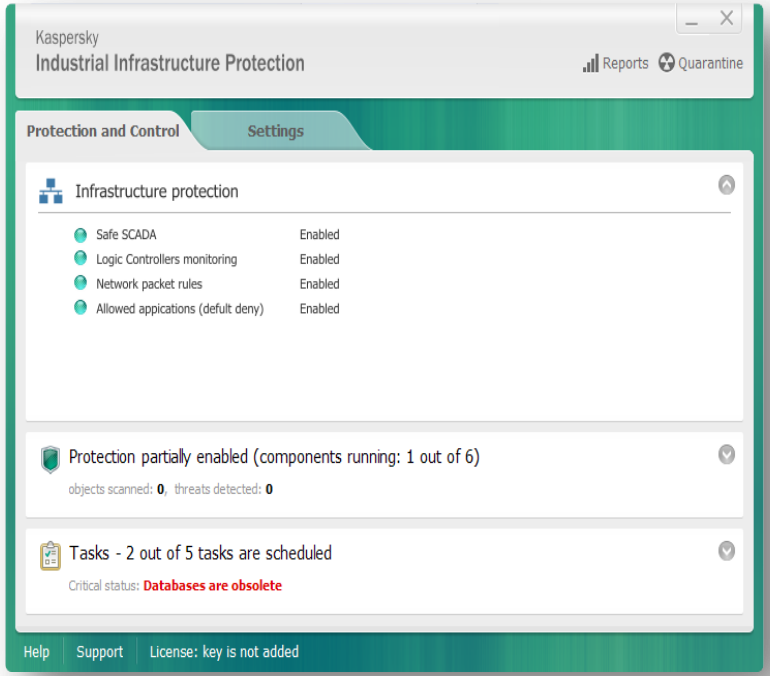
Оценка информационной безопасности, модель угроз, консультации по разработке безопасной системной архитектуры

Облачные технологии защиты

ЗАЩИТЫ РАБОЧИХ СТАНЦИЙ В СРЕДЕ АСУ ТП

Разработано специально для применения в среде АСУ ТП

- Обеспечение замкнутой среды (белые списки)
- Ограничение приложений и устройств
- Определение уязвимостей программной среды
- Режим высокой доступности
- Протоколы взаимодействия с АСУ ТП (HMI, SIEM integration)
- Политика обновлений адаптированная к требованиям АСУ ТП
- Протестировано на совместимость с ПО АСУ ТП

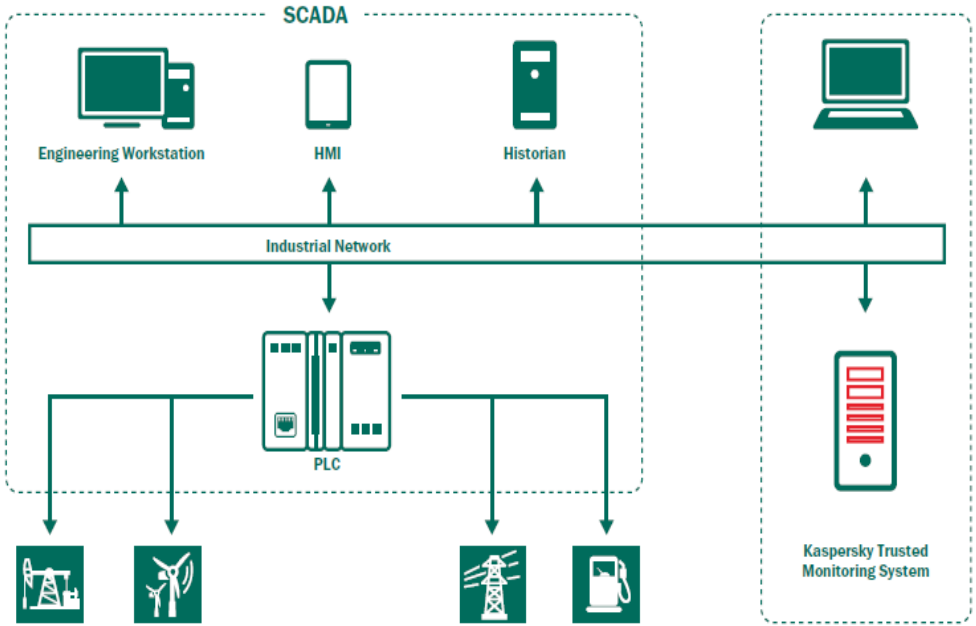


В следующих версиях:

- PLC integrity check
- SafeSCADA technology

ДОВЕРЕННАЯ СИСТЕМА СЕТЕВОГО МОНИТОРИНГА

1. Пассивный мониторинг без влияния на АСУ ТП
2. Анализ сетевого трафика на уровне логики технологического процесса
3. Мониторинг целостности сети
4. Определение появления новых устройств
5. Детектирование подозрительной сетевой активности
6. Поддержка различных индустриальных протоколов
7. Поддержка различных PLC и ПО АСУ ТП



СПАСИБО ЗА ВНИМАНИЕ

KASPERSKY lab