kaspersky

КАК сохранить $1,7 млн. на промышленной кибербезопасности?

Результаты исследования Общего Экономического Эффекта (Total Economic Impact, TEI) от Kaspersky Industrial CyberSecurity проведенного Forrester

Антон Шипулин, Лаборатория Касперского

Обо мне

- Развитие бизнеса промышленной кибербезопасности в **Kaspersky Lab**
- Руководитель программного комитета **Kaspersky Industrial Cybersecurity Conference**
- Координатор международного **Industrial Cybersecurity Center** (**CCI**)
- Сооснователь сообщества специалистов по кибербезопасности АСУ ТП / **RUSCADASEC**
- Certified SCADA Security Architect (**CSSA**), **CISSP**, **CEH**
- @shipulin_anton

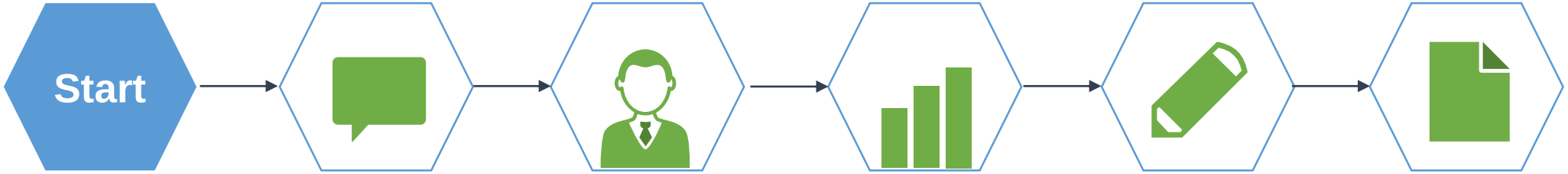
Об исследовании

- Это исследование было заказано «Лабораторией Касперского» и проведено компаний Forrester Consulting. Оно не является инструментом анализа конкурентов.
- Компания Forrester не делает никаких утверждений по поводу окупаемости инвестиций, которая может быть достигнута в других организациях. Компания Forrester настоятельно рекомендует читателям данного документа провести собственную оценку по предлагаемой методике, чтобы определить оправданность вложений в решение KICS.
- «Лаборатория Касперского» ознакомилась с настоящим отчетом и предоставила компании Forrester свои замечания и комментарии, но компания Forrester по-прежнему осуществляет содержательный контроль настоящего отчета и его результатов и не допускает внесения в него изменений, противоречащих результатам исследования и затемняющих его смысл.
- «Лаборатория Касперского» предоставила названия и имена клиентов для проведения опроса, но сама не участвовала в опросе.

Что такое TEI?

		TCO	ROI	TEI
IT impact	IT costs			
	IT cost savings			
Business impact	User efficiency			
	Business effectiveness			
Risk/ uncertainty	Risk mitigation			
	Risk versus reward			
Strategic impact	Scalability			
	Flexibility			

Последовательный подход Forrester для оценки эффекта от Kaspersky Industrial CyberSecurity



Подготовка к исследованию

Интервью с клиентом

Построение финансовой модели

Разработка примера внедрения

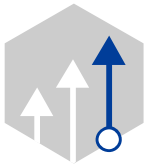
Анализ результата и завершение

Ключевые результаты исследования

Forrester определил следующий трехлетний эффект

На основе анализ обратной связи от заказчика Kaspersky Industrial CyberSecurity и количественных факторов: выгоды, затраты, риски и гибкость

Окупаемость инвестиций
368%



Чистая текущая выгода
1.7 млн долл. США

Срок окупаемости
3 месяца

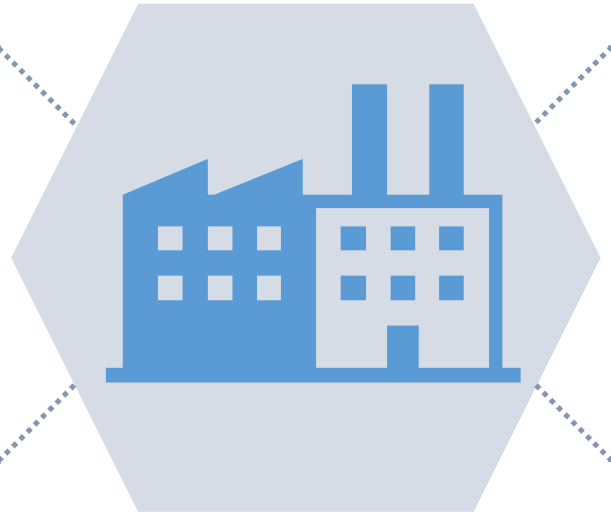
Об исследуемой компании

Отрасль производства

Компания является субъектом критической инфраструктуры и стремится защитить свои объекты от рисков кибератак

Доход 8 млрд долл. США

50 000 сотрудников



Опыт использования KICS

До KICS, использовался устаревший endpoint antivirus где было возможно

Несколько пилотов

После тщательного тестирования выбрали KICS for Nodes

Опыт заказчика до и после использования Kaspersky Industrial CyberSecurity

Ключевые драйверы

- Растущий риск и возможный ущерб от атак на предприятия отрасли клиента
- Специализированное промышленной оборудование и ПО требовало специализированной защиты
- Необходимость соответствия требованиям национального законодательства по кибербезопасности

Требования к решению

- Адекватная защита для рабочих станций включая станции с устаревшими ОС
- Совместимость с ПО и оборудованием компонент систем промышленной автоматизации
- Установка без прерывания промышленных процессов и перезагрузки систем

Ключевые результаты

- Достигнута более качественная защита для компонент систем
- Удобная установка и развертывание обеспечили быструю окупаемость инвестиций
- Отсутствие воздействия на производственный процесс

Мнение клиента до использования KICS for Nodes

“До появления KICS перед нами стояла дилемма: наши рабочие станции могли работать с риском или не работать вообще.”

~Руководитель высшего звена ИБ-департамента, производство

“Нам нужно было решение, которое бы обеспечило эффективную защиту от кибератак и не нарушило непрерывность производства.”

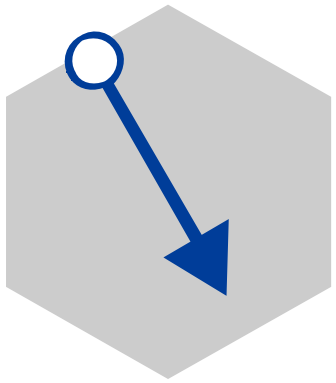
~ Руководитель высшего звена ИБ-департамента, производство

KICS портфолио

Ключевые выгоды от в Kaspersky Industrial CyberSecurity

УСТРАНЕНА СТОИМОСТЬ ВЫНУЖДЕННЫХ ПРОСТОЕВ

Снизили количество и длительность вынужденных простоев из-за блокирования и замедления работы



УСТРАНЕНЫ РАСХОДЫ НА ОБНОВЛЕНИЕ ОС

Устранили необходимость затратного обновления ОС для совместимости с традиционным антивирусом

УСТРАНЕНЫ РАСХОДЫ НА ТРАДИЦИОННЫЙ АНИВИРУС

Отпала необходимость покупки лицензий офисного антивируса

Ключевые выгоды от в Kaspersky Industrial CyberSecurity

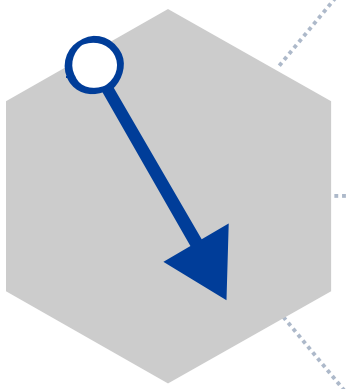
УСТРАНЕНА СТОИМОСТЬ ВЫНУЖДЕННЫХ ПРОСТОЕВ

$1.7 миллионов за три года

- Чтобы хотя бы минимально защитить старое оборудование и иметь возможность обнаруживать кибератаки, организация воспользовалась традиционным антивирусом (не предназначенным для промышленных систем).
- С помощью KICS for Nodes организация смогла защитить уязвимое оборудование, снизив риски кибератак на оборудование и, соответственно, количество и длительность вынужденных простоев.

Доход объекта в час	Средний срок простоев из-за вирусов	Сэкономленные расходы на простои	Поправка на риск
$80,000	10 часов	$800,000	▼15%

УСТРАНЕНЫ РАСХОДЫ НА ОБНОВЛЕНИЕ ОС



Ключевым фактором, мешающим опрошенной организации использовать традиционное антивирусное ПО для конечных точек на рабочих станциях, стала операционная система, установленная на этих компьютерах.

Чтобы должным образом защитить рабочие станции с помощью традиционного антивируса для конечных точек, специалистам по информационной безопасности приходилось обновлять операционные системы до актуальных версий.

Переход на KICS for Nodes избавил организацию от необходимости оплачивать обновление ПО и позволил сохранить необходимый уровень защиты от угроз.

Сэкономленные расходы на обновление ОС	
Расходы на обновление ОС на конечных точках, которых удалось избежать благодаря KICS	$600
Число конечных точек, требующих обновления (за 3 года)	1,050
Сэкономленные расходы на обновление ОС (за 3 года)	$630,000
Поправка на риск	▼10%
Выгода по текущей стоимости за 3 Года	**$461,495**

УСТРАНЕНЫ РАСХОДЫ НА ТРАДИЦИОННЫЙ АНИВИРУС

$49,995 за три года

- Чтобы обеспечить хотя бы минимальный уровень защиты и соответствие отраслевым требованиям, организация установила на этих компьютерах традиционное антивирусное ПО для конечных точек. Успех мероприятия был весьма скромным
- Антивирус блокировал некоторые кибератаки, однако при этом снижалась продуктивность оборудования, блокировались его основные функции, производственные процессы замедлялись или останавливались.
- После перехода на KICS организация перестала использовать традиционное антивирусное ПО для конечных точек на этих рабочих станциях.

Расходы на рабочую станцию/конечную точку, которых удалось избежать благодаря KICS	Число конечных точек (3 года)	Сэкономленные расходы на устаревшее антивирусное ПО для конечных точек	Поправка на риск
$65	1,050	$68,250	▼10%

Неколичественные выгоды Kaspersky Industrial CyberSecurity

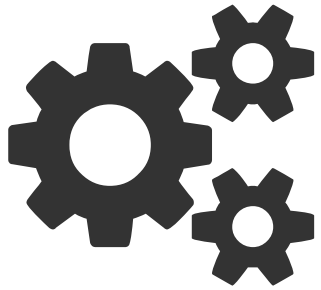
Услуги специалистов по KICS обеспечили дополнительную экспертную поддержку в области аналитики угроз и реагирования на инциденты

Спокойствие и уверенность опрошенных в безопасности инфраструктуры после установки KICS

Анализ затрат на Kaspersky Industrial CyberSecurity

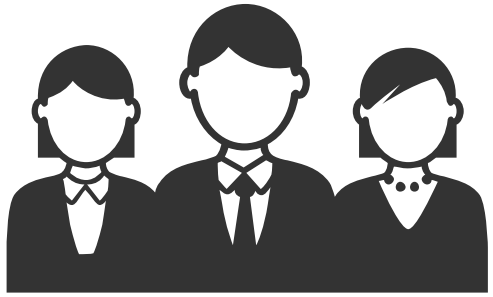
Плата за ПО

Регулярная плата за годовую подписку за все компьютеры



Затраты на внедрение

Участие группы специалистов по контролю информационной безопасности



Операционные затраты на управление

Три FTE (эквивалента полной занятости) тратят 30% своего времени на текущее управление KICS

Исследование TEI также включает факторы гибкости и рисков

ГИБКОСТЬ

Kaspersky дает клиенту возможность реализации дополнительных проектов в будущем

- Использование KICS for Networks с целью повышения прозрачности сети.
- Благодаря KICS for Networks специалисты по информационной безопасности могут выполнять анализ промышленного трафика, выявлять аномалии и устранять уязвимости сети.
- Специалисты также смогли обнаружить изменения параметров в технологических процессах и восстановить их оптимальные значения, обеспечив продуктивную работу оборудования

РИСК ВЛИЯНИЯ НОВОЙ СИСТЕМЫ

Потребности организации, связанные с бизнесом или технологией, не будут удовлетворены за счет внедрения, в результате чего общая выгода будет меньше.

- Уровень риска, который представляют кибератаки, и продолжительность простоев, которых организация планирует избежать с помощью программного обеспечения ICS.
- Стоимость вынужденных простоев.
- Стратегия обновления ОС на компьютерах.

РИСК СВЯЗАННЫЙ С ВНЕДРЕНИЕМ

Отклонение предполагаемого проекта внедрения от первоначальных требований, что может привести к превышению плановых затрат

- Усилия, необходимые для планирования и установки ПО, и число участвующих в процессе FTE (эквивалентов полной занятости).
- График внедрения и увеличение числа компьютеров, защищенных с помощью KICS, с течением времени

Консолидированные показатели за три года с поправкой на риск

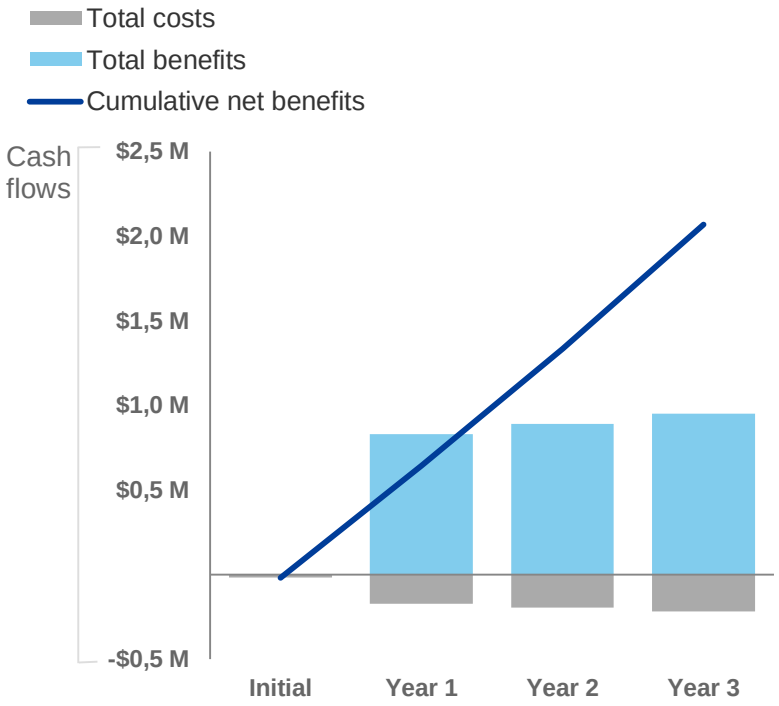
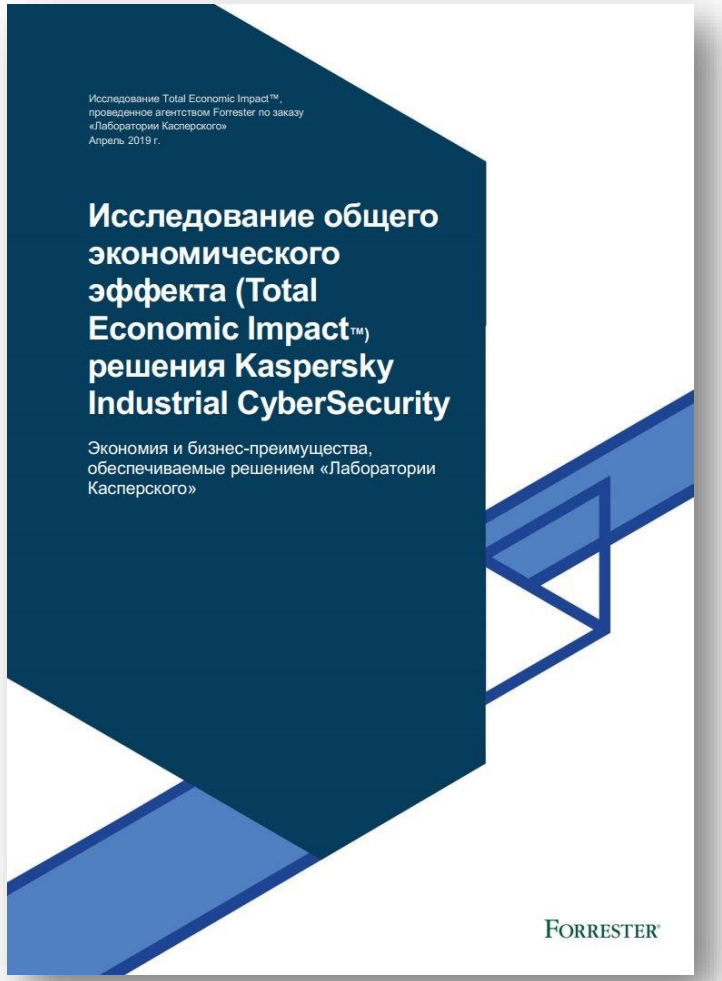
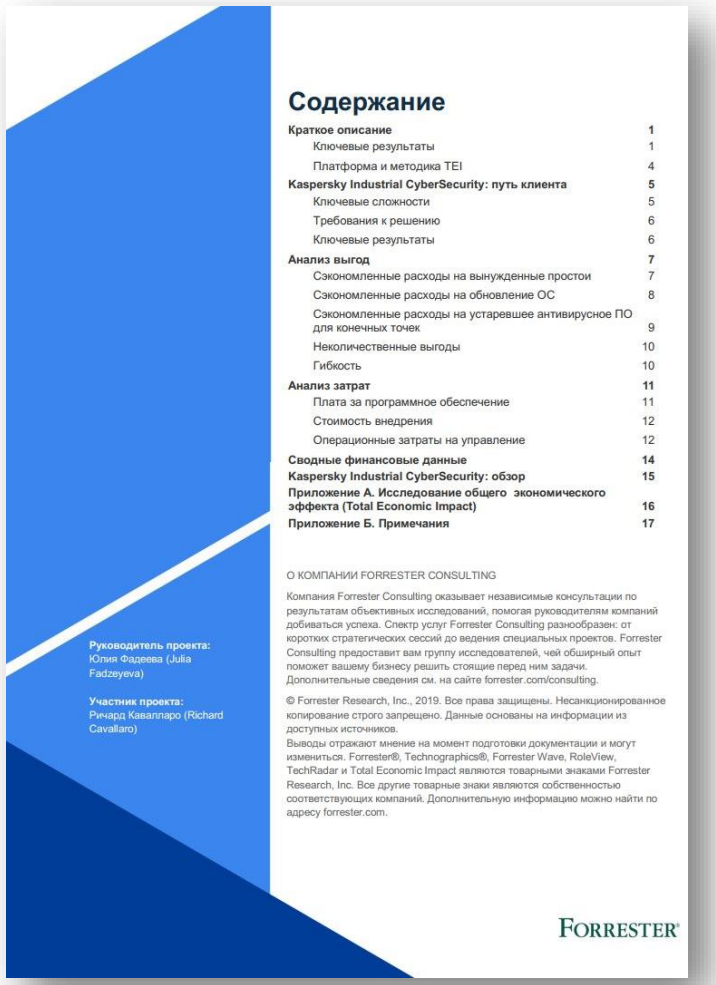


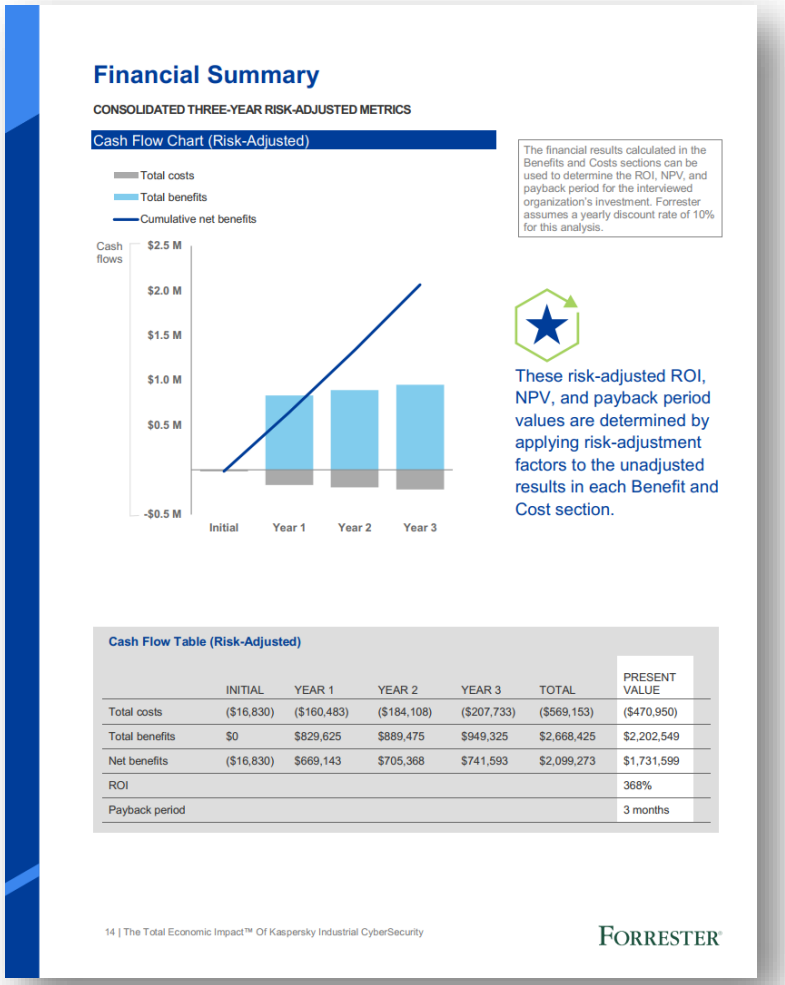
Таблица денежных потоков (с поправкой на риск)

	НАЧАЛО	ГОД 1	ГОД 2	ГОД 3	ВСЕГО	ТЕКУЩАЯ ВЫГОДА
Совокупные затраты, долл. США	(16 830)	(160 483)	(184 10)	(207 733)	(569 153)	(470 950)
Совокупные выгоды, долл. США	0	829 625	889 475	949 325	2 668 425	2 202 549
Чистая выгода, долл. США	16 830	669 143	705 368	741 593	2 099 273	1 731 599
Окупаемость инвестиций						368%
Период окупаемости						3 месяца

Подробный отчет на русском языке







Kaspersky

https://ics.kaspersky.ru/media/Forrester-TEI_Kaspersky-ICS-RU.pdf

kaspersky

Спасибо!

kaspersky.com