

Исследование Total Economic Impact™,
проведенное агентством Forrester по заказу
«Лаборатории Касперского»
Апрель 2019 г.

Исследование общего экономического эффекта (Total Economic Impact™) решения Kaspersky Industrial CyberSecurity

Экономия и бизнес-преимущества,
обеспечиваемые решением «Лаборатории
Касперского»

Содержание

Краткое описание	1
Ключевые результаты	1
Платформа и методика TEI	4
Kaspersky Industrial CyberSecurity: путь клиента	5
Ключевые сложности	5
Требования к решению	6
Ключевые результаты	6
Анализ выгод	7
Сэкономленные расходы на вынужденные простои	7
Сэкономленные расходы на обновление ОС	8
Сэкономленные расходы на устаревшее антивирусное ПО для конечных точек	9
Неколичественные выгоды	10
Гибкость	10
Анализ затрат	11
Плата за программное обеспечение	11
Стоимость внедрения	12
Операционные затраты на управление	12
Сводные финансовые данные	14
Kaspersky Industrial CyberSecurity: обзор	15
Приложение А. Исследование общего экономического эффекта (Total Economic Impact)	16
Приложение Б. Примечания	17

Руководитель проекта:

Юлия Фадеева (Julia Fadzeyeva)

Участник проекта:

Ричард Кавалларо (Richard Cavallaro)

О КОМПАНИИ FORRESTER CONSULTING

Компания Forrester Consulting оказывает независимые консультации по результатам объективных исследований, помогая руководителям компаний добиваться успеха. Спектр услуг Forrester Consulting разнообразен: от коротких стратегических сессий до ведения специальных проектов. Forrester Consulting предоставит вам группу исследователей, чей обширный опыт поможет вашему бизнесу решить стоящие перед ним задачи. Дополнительные сведения см. на сайте forrester.com/consulting.

© Forrester Research, Inc., 2019. Все права защищены. Несанкционированное копирование строго запрещено. Данные основаны на информации из доступных источников.

Выводы отражают мнение на момент подготовки документации и могут измениться. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar и Total Economic Impact являются товарными знаками Forrester Research, Inc. Все другие товарные знаки являются собственностью соответствующих компаний. Дополнительную информацию можно найти по адресу forrester.com.

Преимущества инвестиций



Сэкономленные расходы на вынужденные простои:

1,7 млн долл. США



Сэкономленные расходы на обновление ОС:

461 495 долл. США



Сэкономленные расходы на устаревшее антивирусное ПО для конечных точек:

49 995 долл. США

Краткое описание

Сложность и частота кибератак растут. Согласно данным Национального центра интеграции кибербезопасности и коммуникаций, в последнее время наблюдается общее увеличение количества атак на промышленные системы управления и сбоев в их работе. По мере того как число кибератак увеличивается, количество инцидентов, когда злоумышленникам удалось обойти систему безопасности организации, увеличилось более, чем на 27%: со 102 до 130 инцидентов на организацию в среднем в год. Финансовые убытки от киберпреступности также растут: в 2017 году они составили 10,2 млн долл. США в год в промышленном/производственном секторе. В этой среде многие современные промышленные системы управления (включая те, которые используются в критических инфраструктурных отраслях) до сих пор работают на базе специализированных технологий, что делает их уязвимыми перед различными действиями злоумышленников. Следовательно, специалисты по безопасности ищут специализированные промышленные решения кибербезопасности, чтобы снизить риски, сопряженные с эксплуатацией устаревшей инфраструктуры.

«Лаборатория Касперского» предоставляет решение промышленного уровня для обеспечения кибербезопасности, которое помогает клиентам компании удовлетворять определенные потребности в области кибербезопасности промышленного уровня. Один из компонентов решения — KICS for Nodes — обеспечивает безопасность серверов АСУ ТП, человеко-машинных интерфейсов и рабочих станций от различных киберугроз, причинами которых могут быть человеческий фактор, универсальное вредоносное ПО, целенаправленные атаки или саботаж. Другой компонент — KICS for Networks — функционирует на уровне промышленного протокола связи, анализируя промышленный трафик на предмет аномалий.

Компания «Лаборатория Касперского» поручила компании Forrester Consulting исследовать общий экономический эффект по методике Total Economic Impact™, а также потенциальную рентабельность инвестиций в развертывание решений Kaspersky Industrial CyberSecurity (KICS). Авторы исследования поставили перед собой цель предоставить читателям методику оценки потенциального экономического эффекта от внедрения KICS в организации.

Чтобы лучше понять выгоды, затраты и риски, связанные с инвестицией, компания Forrester опросила одного клиента, который уже несколько лет использует KICS for Nodes и который недавно запустил пилотную программу эксплуатации KICS for Networks.

До внедрения KICS опрошенный клиент пытался обеспечить безопасность устаревших рабочих станций с помощью доступного ПО. Используемое традиционное ПО обеспечивало в лучшем случае ограниченную защиту. Иногда возникали конфликты с программным обеспечением производителя, что обуславливало замедление работы и прерывания производственных процессов.

Ключевые результаты

Количественно выраженная выгода. Опрошенные организации рассчитывают на следующую количественно выраженную выгоду с учетом риска по текущей стоимости:

- › **Сэкономленные расходы на вынужденные простои в объеме 1,7 млн долл. США.** До установки KICS for Nodes в организации не существовало программного обеспечения для эффективной защиты устаревших рабочих станций от кибератак. Организация установила на своем оборудовании временное решение (традиционное антивирусное ПО для конечных точек), которое обеспечивало ограниченную защиту. Иногда, однако, возникали конфликты между установленным решением и легитимным программным обеспечением производителя, приводившие к вынужденным простоям. Кроме того, в организации не была обеспечена полная защита от вирусов, что отрицательно сказывалось на производительности. Благодаря KICS компании удалось защитить уязвимое оборудование, снизить риски кибератак, предотвратить вынужденные простои и избежать замедления работы системы.
- › **Сэкономленные расходы на обновление ОС: 461 495 долл. США.** Без специализированного решения для АСУ ТП организации приходилось пользоваться традиционным антивирусным ПО для конечных точек, чтобы защитить свои рабочие станции. Операционные системы (ОС), установленные на производственном оборудовании, часто были несовместимы с антивирусным решением для конечных точек. Чтобы антивирусное ПО работало должным образом, специалистам по информационной безопасности требовалось выполнять требующие значительных средств и времени обновления ОС на этих рабочих станциях. Переход на KICS for Nodes избавил организацию от необходимости выполнять дорогостоящие обновления ПО и позволил сохранить необходимый уровень защиты от угроз.
- › **Сэкономленные расходы на устаревшее антивирусное ПО для конечных точек: 49 995 долл. США.** Чтобы обеспечить базовую защиту и соответствие отраслевым требованиям, на рабочих станциях организации было выборочно установлено традиционное антивирусное ПО для рабочих точек. Антивирус блокировал некоторые вирусные атаки, однако при этом снижалась продуктивность оборудования, блокировались его основные функции, производственные процессы замедлялись или останавливались. После перехода на KICS организации больше не требовалось использовать традиционное антивирусное ПО для конечных точек на рабочих станциях и оплачивать лицензии для этих машин.

Неколичественные выгоды. Опрошенные организации отметили следующие выгоды, которые в рамках этого исследования не были оценены количественно:

- › **Услуги специалистов «Лаборатории Касперского» обеспечили дополнительную экспертную поддержку в области аналитики угроз и реагирования на инциденты.** Несмотря на то что опрошенной организации не пришлось прибегать к услугам специалистов по KICS на момент интервью, компания знает, что для получения помощи от «Лаборатории Касперского» достаточно одного телефонного звонка.
- › **Спокойствие.** Невозможно в цифрах оценить уверенность опрошенных в безопасности инфраструктуры после установки KICS. Опрошенные уверены, что после внедрения специализированного ПО промышленные системы будут лучше защищены. Специалисты по информационной безопасности снизили совокупные риски нарушений безопасности в организации.



Окупаемость инвестиций
368%



Общая выгода (текущая стоимость)
2,2 млн долл. США



Чистая текущая стоимость
1,7 млн долл. США



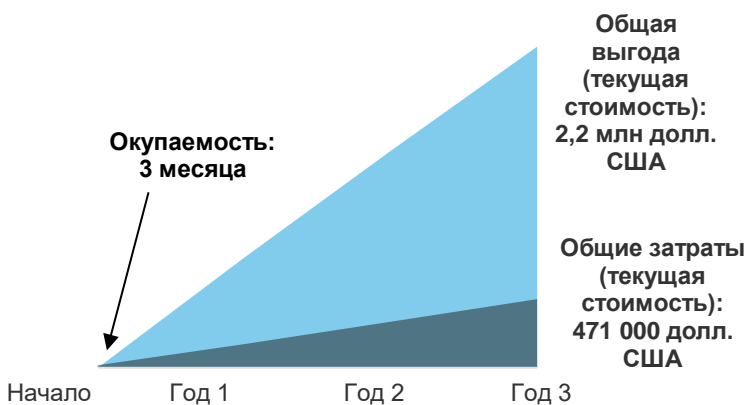
Окупаемость
3 месяца

Затраты. Опрошенная организация рассчитывает на следующие расходы (текущая стоимость) с учетом риска:

- › **Плата за программное обеспечение.** Организация оплачивала стоимость лицензий на ПО KICS for Nodes на три года на общую сумму 201 904 долл. США по текущей стоимости.
- › **Затраты на внедрение.** Организация назвала процедуру внедрения удобной и беспроблемной. Следуя своему стратегическому плану, опрошенная компания постепенно установила KICS for Nodes на 450 компьютерах. Включая усилия по планированию и утверждению внедрения совокупная стоимость миграции (в эквиваленте чистой выгоды за три года с поправкой на риск) составила 25 310 долл. США.
- › **Операционные затраты на управление.** Опрошенная организация назначила три работающих на полную смену специалистов по информационной безопасности, чтобы те занимались управлением KICS примерно 30% своего рабочего времени. На это организация за три года потратила сумму 243 736 долл. США в эквиваленте чистой выгоды.

Интервью Forrester с существующим клиентом и последующий финансовый анализ Forrester показали, что выгоды опрошенной организации составляют 2,2 млн долл. США за три года, а затраты за аналогичный период — 470 950 млн долл. США, то есть чистая текущая выгода равна 1,7 млн долл. США, а рентабельность инвестиций — 368%.

Сводные финансовые данные



Выгоды за три года

Сэкономленные расходы на антивирусное ПО для устаревших конечных точек: 49 995 долл. США

Сэкономленные расходы на обновление ОС: 461 495 долл. США



Сэкономленные расходы на вынужденные простои: 1 691 059 долл. США

Методика ТЕІ помогает компаниям продемонстрировать, обосновать и реализовать материальную выгоду предлагаемых ИТ-проектов как перед высшим руководством компании, так и перед другими заинтересованными участниками бизнеса.

Платформа и методика ТЕІ

По результатам бесед компания Forrester составила методику анализа общего экономического эффекта (Total Economic Impact™, ТЕІ) для организаций, рассматривающих возможность внедрения Kaspersky Industrial CyberSecurity.

Назначение этой платформы — выявление факторов, влияющих на инвестиционное решение, а именно затрат, выгод, гибкости и рисков. Компания Forrester использовала многоступенчатый процесс для оценки возможного экономического эффекта от внедрения решения KICS в организации.



ПОДГОТОВКА К ИССЛЕДОВАНИЮ

Опрошены эксперты «Лаборатории Касперского» и аналитики Forrester, чтобы собрать данные о решении.



ИНТЕРВЬЮ С КЛИЕНТОМ

Проведен опрос представителей одной организации, использующей KICS, чтобы получить данные о затратах, выгодах и рисках.



ФИНАНСОВАЯ МОДЕЛЬ

По результатам опроса с использованием методики ТЕІ была создана финансовая модель с учетом рисков на основе проблем и задач, отмеченных в ходе исследования представителями опрошенных организаций.



ПРИМЕР ВНЕДРЕНИЯ

Для построения модели влияния KICS использовались четыре основных элемента ТЕІ: выгоды, затраты, гибкость и риски. Анализ рентабельности инвестиций в ИТ, который приходится проводить организациям, постоянно усложняется. Методика ТЕІ, разработанная компанией Forrester, позволяет представить полную картину общего экономического эффекта от принимаемых решений по закупке. Дополнительную информацию о методике ТЕІ см. в приложении А.

РАСКРЫВАЕМЫЕ СВЕДЕНИЯ

Читателям следует помнить следующее:

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.

Kaspersky Industrial CyberSecurity: путь клиента

ДО И ПОСЛЕ ИНВЕСТИРОВАНИЯ В KICS

Опрошенная организация

В контексте этого исследования компания Forrester опросила одного из клиентов KICS:

- › Специалисты Forrester провели интервью с двумя старшими специалистами команды по информационной безопасности.
- › Клиент — крупная производственная компания с центральным офисом в России. Доход компании в 2018 году согласно отчетности превысил 8 млрд долл. США, а на ее объектах в разных странах мира работает более 50 000 сотрудников.
- › Компания имеет дело с критически важной инфраструктурой, поэтому вопросы безопасности и защиты объектов от угрозы кибератак имеют для нее приоритетное значение.
- › Переоценка своих программ безопасности позволила организации осознать необходимость в новой антивирусной системе для защиты рабочих станций, так как традиционные антивирусы для конечных точек не защищали их или защищали недостаточно.
- › Организация провела несколько проверок концепции с несколькими поставщиками специализированного ПО для обеспечения промышленной кибербезопасности и по результатам жесткого отбора выбрала решение KICS for Nodes. Мысля стратегически, специалисты организации выбрали, на каких рабочих станциях новое ПО нужно установить в первую очередь, и модернизировали их за пару лет.

На момент интервью организация выбирала поставщика для обеспечения сетевой безопасности и не могла предоставить финансовые показатели использования KICS for Networks. Однако на момент публикации компания приняла решение о развертывании KICS for Networks.

Ключевые сложности

Опрошенная организация рассказала о следующих проблемах, стимулирующих факторах, задачах, целях и возможностях:

- › **Из-за растущих рисков и огромных убытков от кибератак на промышленные системы вопрос промышленной кибербезопасности стал приоритетным.** За последние несколько лет число кибератак в организациях, работающих с ключевой инфраструктурой, увеличилось.¹ Несмотря на то что в опрошенной организации до сих пор не было серьезных кибератак, она видела, как другие компании на рынке страдают от киберпреступности. Возможность значительной потери прибыли, физических убытков и вреда, а также потенциальная угроза национальной безопасности заставили специалистов по безопасности действовать решительно.

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

*Руководитель высшего звена
ИБ-департамента,
производство*



- › **Специализированному производственному оборудованию требовалась защита промышленного уровня, обеспечить которую с помощью традиционного антивирусного ПО для конечных точек было невозможно.** В отсутствие специализированного ICS-решения опрошенная организация пользовалась традиционным антивирусом для конечных точек, чтобы обеспечить безопасность своих рабочих станций. Это программное обеспечение не предназначено для промышленных систем, поэтому оно обеспечивает ограниченную защиту и иногда вступает в конфликт со специализированным ПО, прерывая производственный процесс.
- › **Как и любая другая компания, работающая с критически важной инфраструктурой, опрошенная организация обязана соблюдать государственные требования в области кибербезопасности.** Опрошенная организация осознает необходимость изменить использовавшийся ранее подход к кибербезопасности, чтобы обеспечить соответствие нормативным требованиям. Для этого требовалось специализированное ICS-решение.

Требования к решению

Опрошенная организация предъявляла следующие требования к новому решению:

- › Эффективная защита рабочих станций, включая машины с более старыми версиями ОС.
- › Совместимость с программными и аппаратными компонентами промышленных систем автоматизации.
- › Возможность установки без прерывания производственного процесса и без перезагрузки системы.
- › Низкие требования к влиянию на производительность и ресурсы.

Ключевые результаты

Опрошенные назвали несколько результатов вложения средств в KICS:

- › **Организация смогла лучше защитить свои промышленные системы.** Решение KICS позволило опрошенной организации защитить рабочие станции, которые в противном случае остались бы без защиты или с традиционным антивирусом для конечных точек, который в лучшем случае обеспечивал ограниченную защиту.
- › **Внедрение этого нересурсоемкого решения никак не повлияло на производственный процесс.** Решение KICS for Nodes не истощало ресурсы компьютеров, а его установка не привела к перерывам в работе объекта или замедлению его деятельности.
- › **Удобная установка и развертывание обеспечили быструю окупаемость инвестиций.** Беспроблемная установка позволила организации установить на рабочих станциях KICS for Nodes без перезагрузки систем или остановки производства.

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

*Руководитель высшего звена
ИБ-департамента,
производство*



«Сейчас мы на раннем этапе внедрения системы промышленной кибербезопасности и еще не используем весь потенциал KICS. Мы уже осознаем ценность этого продукта и видим, как с его помощью удастся снизить риски для компании, поэтому мы планируем расширять его развертывание и в будущем использовать все возможности продукта».

*Руководитель высшего звена
ИБ-департамента,
производство*



Анализ выгод

ДАННЫЕ О КОЛИЧЕСТВЕННЫХ ВЫГОДАХ

Общая выгода (долл. США)

№	ВЫГОДА	ГОД 1	ГОД 2	ГОД 3	ВСЕГО	ТЕКУЩАЯ ВЫГОДА
Atr	Сэкономленные расходы на вынужденные простои	680 000	680 000	680 000	2 040 000	1 691 059
Btr	Сэкономленные расходы на обновление ОС	135 000	189 000	243 000	567 000	461 495
Ctr	Сэкономленные расходы на антивирусное ПО для традиционных конечных точек	14 625	20 475	26 325	61 425	49 995
	Общая выгода (с поправкой на риск)	829 625	889 475	949 325	2 668 425	2 202 549

Сэкономленные расходы на вынужденные простои

Одним из основных преимуществ использования KICS опрошенная организация называет защиту от вынужденных простоев. Простои промышленного предприятия — это чаще всего финансовые убытки, потерянный доход, снижение продуктивности сотрудников, недовольство клиентов и ущерб для репутации. Любой незапланированный простой требует расследования и дополнительных усилий на восстановление деятельности.

Согласно опрошенным лицам:

- › Чтобы хотя бы минимально защитить старое оборудование и иметь возможность обнаруживать кибератаки, организация воспользовалась традиционным антивирусным решением для конечных точек (не предназначенным для промышленных систем). Программное обеспечение функционировало с переменным успехом, но иногда блокировало вполне безобидные операции, являющиеся частью производственного процесса. В результате производственные системы приходилось останавливать до устранения причины проблем.
- › Периодически организация обнаруживала вирусы, которые не останавливали, но существенно замедляли ее работу или блокировали функционирование отдельных систем, что не могло не сказаться на производительности.

С помощью KICS for Nodes организация смогла защитить уязвимое оборудование, снизив риски кибератак на оборудование и, соответственно, количество и длительность вынужденных простоев.

В контексте данного исследования Forrester делает следующие допущения:

- › Средняя продолжительность простоев из-за вирусов на производственном предприятии, аналогичном опрошенной организации, равна 10 часов в год.
- › Доход объекта в час равен 80 000 долл. США (при условии работы объекта в круглосуточном режиме без выходных).

Эта выгода будет варьироваться в зависимости от следующих

7 | Исследование общего экономического эффекта (Total Economic Impact™) решения Kaspersky Industrial CyberSecurity

В таблице выше показана общая выгода в перечисленных ниже областях, а также текущая стоимость с дисконтом 10%. Ожидаемая общая выгода опрошенной организации в течение трех лет составляет свыше 2,2 млн. долл. США с учетом риска.



Сэкономленные расходы на вынужденные простои: **77%** общей выгоды

факторов:

- › Уровень риска, который представляют кибератаки, и продолжительность простоев, которых организация планирует избежать с помощью программного обеспечения ICS.
- › Стоимость вынужденных простоев.

Чтобы учесть эти риски, специалисты Forrester уменьшили ожидаемую выгоду на 15%, что дало текущую выгоду за три года с учетом рисков в размере 1 691 059 долл. США.

«Риск, связанный с влиянием новой системы» означает вероятность того, что потребности организации, связанные с бизнесом или технологией, не будут удовлетворены за счет внедрения, в результате чего общая выгода будет меньше. Чем больше неопределенность, тем шире потенциальный диапазон результатов оценки выгод.

Сэкономленные расходы на вынужденные простои: таблица расчетов

№	ПОКАЗАТЕЛЬ	РАСЧЕТ	ГОД 1	ГОД 2	ГОД 3
A1	Доход от объекта в час, долл. США		80 000	80 000	80 000
A2	Продолжительность простоев из-за вирусов в год в часах, которых удалось избежать благодаря KICS		10	10	10
At	Сэкономленные расходы на вынужденные простои, долл. США	A1*A2	800 000	800 000	800 000
	Поправка на риск	↓15%			
Atr	Сэкономленные расходы на вынужденные простои (с поправкой на риск), долл. США		680 000	680 000	680 000

Сэкономленные 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. Версии операционных систем (ОС), установленных на производственном оборудовании, часто были несовместимы с доступным антивирусом. Чтобы должным образом защитить рабочие станции с помощью традиционного антивируса для конечных точек, специалистам по информационной безопасности приходилось обновлять операционные системы до актуальных версий. Организации такое обновление обходилось в среднем в 600 долл. США на рабочую станцию.

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

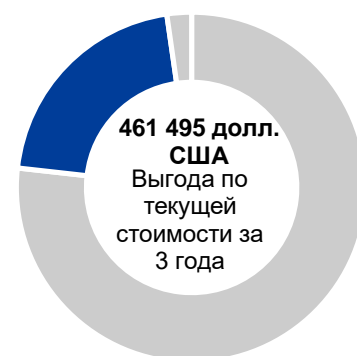
Для целей исследования компания Forrester сделала следующие допущения:

- › Организация внедряла новое решение постепенно. В течение первого года компания установила KICS for Nodes на 250 компьютерах, расширила покрытие до 350 рабочих станций в течение 2 года и 450 компьютеров в течение 3 года. Таким образом потребность в обновлении ОС была устранена.
- › На обновлении ОС компании удалось сэкономить 600 долл. США с рабочей станции.

Сэкономленные расходы на обновление ПО будут варьироваться в зависимости от следующих факторов:

- › Стратегия обновления ОС на компьютерах.
- › Средняя стоимость обновления операционной системы.

Чтобы учесть эти риски, специалисты Forrester уменьшили



Сэкономленные расходы на обновление ОС: 21% общей выгоды

ожидаемую выгоду на 10%, что дало текущую выгоду за три года с учетом рисков в размере 461 495 долл. США.

Сэкономленные расходы на обновление ОС: таблица расчетов

№	ПОКАЗАТЕЛЬ	РАСЧЕТ	ГОД 1	ГОД 2	ГОД 3
B1	Расходы на обновление ОС на конечных точках, которых удалось избежать благодаря KICS, долл. США		600	600	600
B2	Число конечных точек, требующих обновления		250	350	450
Bt	Сэкономленные расходы на обновление ОС, долл. США	$B1 \cdot B2$	150 000	210 000	270 000
	Поправка на риск	↓10%			
Btr	Сэкономленные расходы на обновление ОС (с поправкой на риск), долл. США		135 000	189 000	243 000

Сэкономленные расходы на устаревшее антивирусное ПО для конечных точек

Опрошенная организация стремилась обеспечить эффективную антивирусную защиту на определенных рабочих станциях ввиду значительного возраста оборудования или установленных операционных систем. 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.

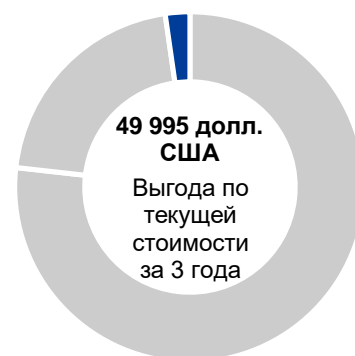
Для целей исследования компания Forrester сделала следующие допущения:

- › Организация внедряла новое решение постепенно. В течение первого года она заменила традиционное антивирусное ПО для конечных точек решением KICS for Nodes на 250 компьютерах, расширила покрытие до 350 рабочих станций в течение 2 года и 450 компьютеров в течение 3 года.
- › Стоимость лицензии на традиционное антивирусное ПО для конечных точек составляет 65 долл. США в год.

Сокращение затрат на офисное антивирусное ПО будет варьироваться в зависимости от следующих факторов:

- › Число рабочих станций, обновляемых до KICS ежегодно.
- › Стоимость одной лицензии на традиционное антивирусное ПО для конечных точек.

Чтобы учесть эти риски, специалисты Forrester уменьшили ожидаемую выгоду на 10%, что дало текущую выгоду за три года с учетом рисков в размере 49 995 долл. США.



Сэкономленные расходы на антивирусное ПО для устаревших конечных точек: 2% общей выгоды

Сэкономленные расходы на устаревшее антивирусное ПО для конечных точек: таблица расчетов

№	ПОКАЗАТЕЛЬ	РАСЧЕТ	ГОД 1	ГОД 2	ГОД 3
C1	Расходы на рабочую станцию/конечную точку, которых удалось избежать благодаря KICS, долл. США		65	65	65
C2	Число конечных точек		250	350	450
Ct	Сэкономленные расходы на устаревшее антивирусное ПО для конечных точек, долл. США	$C1 \cdot C2$	16 250	22 750	29 250
	Поправка на риск	↓10%			
Ctr	Сэкономленные расходы на антивирусное ПО для устаревших конечных точек (с поправкой на риск), долл. США		14 625	20 475	26 325

Неколичественные выгоды

- Услуги специалистов по KICS обеспечили дополнительную экспертную поддержку в области аналитики угроз и реагирования на инциденты.** Несмотря на то что с момента установки KICS for Nodes опрошенной организации не потребовались услуги «Лаборатории Касперского», она знает, что для получения помощи от специалистов по кибербезопасности достаточно одного телефонного звонка.
- Спокойствие.** Невозможно в цифрах оценить уверенность опрошенных в безопасности инфраструктуры после установки KICS. Они знают, что после внедрения специализированного ПО промышленные системы будут лучше защищены. Специалисты по информационной безопасности снизили совокупные риски нарушений безопасности в организации.

Гибкость

Очевидно, что величина гибкости совершенно уникальна для каждого клиента, как впрочем и ее оценка каждой организацией. Во многих случаях заказчик может выбрать внедрение KICS и позднее выявить дополнительные выгоды и бизнес-возможности, включая следующее:

- Использование KICS for Networks с целью повышения прозрачности сети.** На момент проведения опроса организация использовала KICS for Networks в пилотном режиме и наблюдала положительные результаты. Благодаря продукту «Лаборатории Касперского» специалисты по информационной безопасности могут выполнять анализ промышленного трафика, выявлять аномалии и устранять уязвимости сети. С помощью KICS for Networks специалисты также смогли обнаружить изменения параметров в технологических процессах и восстановить их оптимальные значения, обеспечив продуктивную работу оборудования.

Гибкость также получает количественную оценку при рассмотрении конкретного проекта (этот процесс описан более подробно в приложении А).



Опрошенные были уверены, что после внедрения KICS промышленные системы будут лучше защищены. Специалисты по информационной безопасности снизили совокупные риски нарушений безопасности в организации.

Гибкость в методике TEI означает инвестиции в расширение бизнес-возможностей или производственных мощностей, которые могут принести выигрыш в результате некоторых дополнительных инвестиций в будущем. Они дают организации «право» или возможность реализации проектов в будущем, но не обязывают ее это делать.

Анализ затрат

КОЛИЧЕСТВЕННЫЕ ДАННЫЕ ЗАТРАТ

Совокупные затраты (долл. США)

№	ЗАТРАТЫ	НАЧАЛО	ГОД 1	ГОД 2	ГОД 3	ВСЕГО	ТЕКУЩАЯ ВЫГОДА
Dtr	Плата за программное обеспечение	0	59 063	82 688	106 313	248 063	201 904
Etr	Затраты на внедрение	16 830	3 410	3 410	3 410	27 060	25 310
Ftr	Операционные затраты на управление	0	98 010	98 010	98 010	294 030	243 736
	Совокупные затраты (с поправкой на риск)	16 830	160 483	184 108	207 733	569 153	470 950

Плата за программное обеспечение

Организация потратила средства на приобретение лицензий на ПО Kaspersky Industrial CyberSecurity. Это регулярная плата за годовую подписку в зависимости от числа компьютеров, безопасность которых обеспечивает KICS.

В течение первого года организация оплатила ПО для 250 машин, затем добавила еще по 100 лицензий в третий и четвертый годы, увеличив общее число лицензий до 450.

«Лаборатория Касперского» предоставила реалистичные данные, и агентство Forrester скорректировало их на 5% с учетом рисков, чтобы учесть скидки за объем). За три года совокупные затраты (текущая стоимость) составили 201 904 долл. США.

В таблице выше показаны совокупные затраты в перечисленных ниже областях, а также текущая стоимость с дисконтом 10%. Ожидаемые совокупные затраты опрошенной организации в течение трех лет составляют 470 950 долл. США (по текущей стоимости) с учетом риска.

Связанный с внедрением риск — это риск, связанный с вероятностью отклонения предполагаемого проекта внедрения от первоначальных требований, что может привести к превышению плановых затрат. Чем больше неопределенность, тем шире потенциальный диапазон результатов оценки затрат.

Плата за программное обеспечение: таблица расчетов

№	ПОКАЗАТЕЛЬ	РАСЧЕТ	НАЧАЛО	ГОД 1	ГОД 2	ГОД 3
D1	Стоимость KICS for Nodes на каждую машину, долл. США			225	225	225
D2	Число конечных точек (машин)			250	350	450
Dt	Плата за программное обеспечение, долл. США	$D1 \cdot D2$	0	56 250	78 750	101 250
	Поправка на риск	↑5%				
Dtr	Плата за ПО (с учетом рисков), долл. США		0	59 063	82 688	106 313

Стоимость внедрения

Опрошенная организация описала внедрение KICS for Nodes как процесс, который потребовал следующего:

- › Участие группы специалистов по контролю информационной безопасности в течение 150 часов для планирования первоначального внедрения. Так как организация постепенно увеличивала число установленных экземпляров KICS, специалисты Forrester добавили еще 10 часов на планирование в течение лет после первоначального внедрения.
- › Участие специалистов по контролю кибербезопасности, которые изначально потратили 100 часов на установку KICS for Nodes на компьютеры. По консервативным оценкам Forrester в последующие годы специалисты потратили 50 часов на расширение внедрения.

Затраты на внедрение будут варьироваться в зависимости от следующих факторов:

- › 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.
- › Размер почасовой оплаты труда специалистов, участвующих во внедрении.

Чтобы учесть эти риски, специалисты Forrester увеличили ожидаемые затраты на 10%, что дало текущую выгоду с учетом рисков за три года в размере 25 310 долл. США.



250 часов
было потрачено на
первоначальное
планирование и
развертывание

Стоимость внедрения: таблица расчетов

№	ПОКАЗАТЕЛЬ	РАСЧЕТ	НАЧАЛО	ГОД 1	ГОД 2	ГОД 3
E1	Продолжительность планирования (ч)		150	10	10	10
E2	Средний размер оплаты труда менеджера по информационной безопасности (почасовая, с учетом всех обязательств работодателя), долл. США		70	70	70	70
E3	Продолжительность внедрения (ч)		100	50	50	50
E4	Средний размер оплаты труда аналитика информационной безопасности (почасовая, с учетом всех обязательств работодателя), долл. США		48	48	48	48
Et	Затраты на внедрение	$E1 * E2 + E3 * E4$	15 300	3 100	3 100	3 100
	Поправка на риск	↑10%				
Etr	Затраты на внедрение (с учетом риска), долл. США		16 830	3 410	3 410	3 410

Операционные затраты на управление

Опрошенная организация назначила трех работающих на полную ставку аналитиков информационной безопасности для управления KICS for Nodes. В среднем, они уделяли этому 30% своего рабочего времени.

Операционные затраты на управление KICS могут варьироваться в зависимости от следующих факторов:

- › Широта внедрения KICS.
- › Число инцидентов, требующих расследования на постоянной основе.
- › Годовые зарплаты аналитиков информационной безопасности с учетом всех обязательств работодателя.

Чтобы учесть эти риски, специалисты Forrester увеличили ожидаемые затраты на 10%, что дало текущую выгоду с учетом рисков за три года в размере 243 736 долл. США.



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

Операционные затраты на управление: таблица расчетов

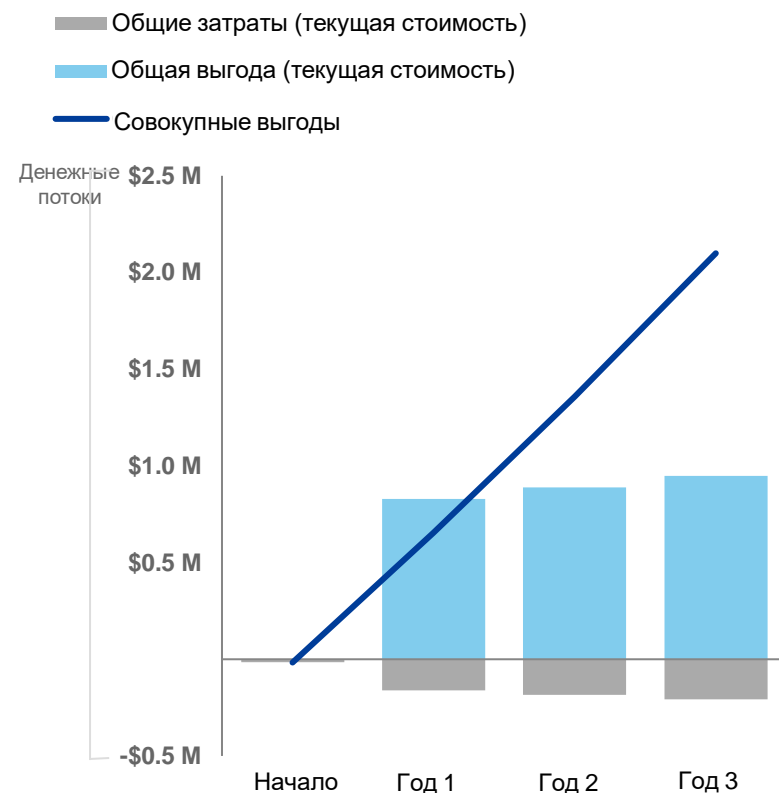
№	ПОКАЗАТЕЛЬ	РАСЧЕТ	НАЧАЛО	ГОД 1	ГОД 2	ГОД 3
F1	Аналитики информационной безопасности, занятые управлением KICS			3	3	3
F2	Процент рабочего времени аналитиков, расходуемого на управление KICS			30%	30%	30%
F3	Средняя годовая зарплата (со всеми обязательствами работодателя) аналитика информационной безопасности, долл. США			99 000	99 000	99 000
Ft	Текущее управление KICS, долл. США	$F1 \cdot F2 \cdot F3$	0	89 100	89 100	89 100
	Поправка на риск	↑10%				
Ftr	Операционные затраты управление (с поправкой на риск), долл. США		0	98 010	98 010	98 010

Внутренние затраты на обучение специалистов по информационной безопасности работе с KICS Forrester считает несущественными. В рамках пилотного этапа небольшая группа аналитиков информационной безопасности опрошенной организации обучились работе с KICS за один день. Никаких дополнительных программ обучения по окончании пилотного этапа не проводилось.

Сводные финансовые данные

КОНСОЛИДИРОВАННЫЕ ПОКАЗАТЕЛИ ЗА ТРИ ГОДА С ПОПРАВКОЙ НА РИСК

Диаграмма денежного потока (с поправкой на риск)



Финансовые результаты, полученные в разделах «Затраты» и «Выгода», можно использовать для вычисления рентабельности, чистой текущей стоимости и периода окупаемости в отношении инвестиций опрошенных организаций. В данном исследовании компания Forrester использовала процентную ставку, равную 10%.



Рентабельность инвестиций, чистая текущая выгода и период окупаемости с поправкой на риск получены применением коэффициентов поправки на риск к исходным результатам, представленным в разделах с описанием затрат или выгод.

Таблица денежных потоков (с поправкой на риск)

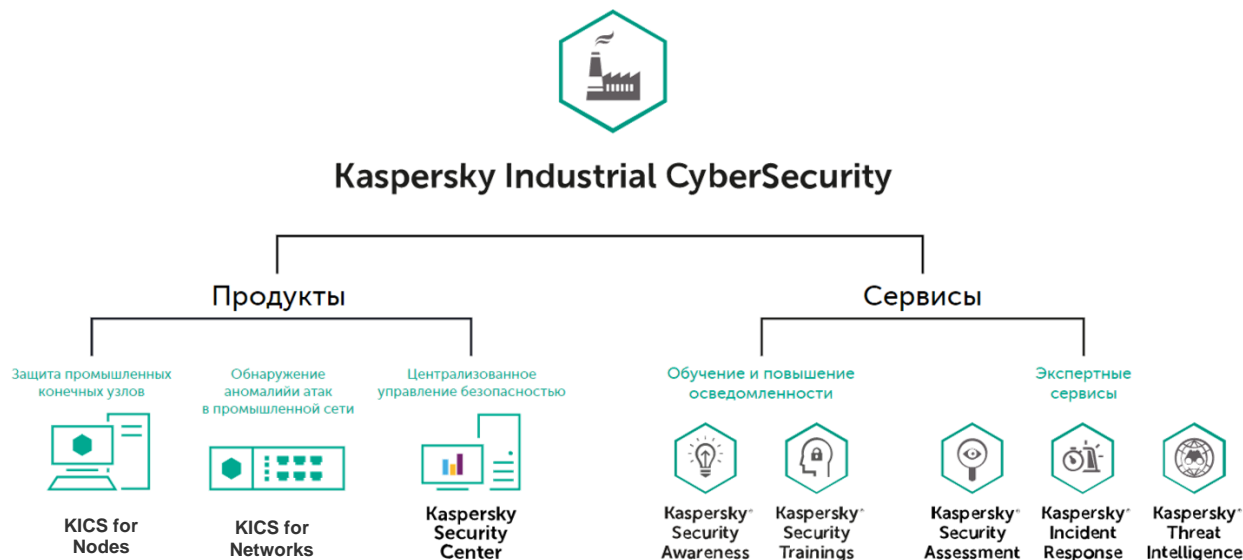
	НАЧАЛО	ГОД 1	ГОД 2	ГОД 3	ВСЕГО	ТЕКУЩАЯ ВЫГОДА
Совокупные затраты, долл. США	(16 830)	(160 483)	(184 10)	(207 733)	(569 153)	(470 950)
Совокупные выгоды, долл. США	0	829 625	889 475	949 325	2 668 425	2 202 549
Чистая выгода, долл. США	16 830	669 143	705 368	741 593	2 099 273	1 731 599
Окупаемость инвестиций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

Kaspersky Industrial CyberSecurity: обзор

Следующая информация предоставлена «Лабораторией Касперского». Forrester не проверяет какие-либо заявления «Лаборатории Касперского» и не рекламирует саму компанию или предлагаемые ей решения.

Kaspersky Industrial CyberSecurity (KICS) — это портфель продуктов и услуг, предназначенных для удовлетворения уникальных потребностей промышленных сред.

Комплексный подход «Лаборатории Касперского» помогает клиенту на каждом этапе процесса обеспечения кибербезопасности промышленной среды: от оценки кибербезопасности до реагирования на инциденты.



KICS for Nodes представляет собой продукт для защиты конечных точек промышленного уровня. Он помогает защитить конечные точки промышленной системы управления, включая серверы SCADA, рабочие станции и многое другое.

KICS for Networks представляет собой решение для обнаружения аномалий, атак и нарушений безопасности в промышленных сетях. Оно отслеживает сетевой трафик и обеспечивает безопасность сетевого уровня, реализованную на уровне промышленного протокола связи.

Экспертные услуги включают оценку промышленной кибербезопасности, тестирование на возможность проникновения в систему, реагирование на инциденты и аналитику угроз.

Программы обучения включают базовое обучение промышленной кибербезопасности для топ-менеджеров, инженеров, а также обучение экспертного уровня для специалистов по ИТ/ОТ-безопасности.

Подробнее на сайте: <https://ics.kaspersky.ru>

Связаться: ics@kaspersky.com

Приложение А. Исследование общего экономического эффекта (Total Economic Impact)

Total Economic Impact — это методика, разработанная агентством Forrester Research, которая позволяет оптимизировать процесс принятия решений в сфере технологий и помогает поставщикам довести информацию о ценности своих продуктов и услуг до сведения клиентов. Методика ТЕІ помогает компаниям продемонстрировать, обосновать и реализовать материальную выгоду предлагаемых ИТ-проектов как перед высшим руководством компании, так и перед другими заинтересованными участниками бизнеса.

Подход к исследованию общего экономического эффекта (Total Economic Impact)



Выгода — это ценность, которую получил бизнес благодаря продукту. Методика ТЕІ придает одинаковое значение оценке выгод и оценке затрат. Это позволяет полностью исследовать влияние данной технологии на работу организации в целом.



Общая сумма затрат учитывает все инвестиции и расходы, необходимые для получения предполагаемой ценности (или выгод) продукта. Категория затрат по методике ТЕІ учитывает любые дополнительные затраты и накладные расходы в существующей среде, связанные с данным решением.



Гибкость в методике ТЕІ означает стратегическую ценность, которую можно получить в результате некоторых дополнительных инвестиций в будущем на основе первоначальных, уже сделанных инвестиций. Возможность реализовать данную выгоду в будущем также имеет определенную текущую выгоду, которая может быть оценена.



Понятие риска служит для измерения неопределенности при оценке затрат и выгоды с учетом следующего: 1) вероятность того, что расчеты будут соответствовать первоначальным оценкам, или 2) вероятность того, что оценки будут отслеживаться на протяжении определенного периода времени. Коэффициенты риска по методике ТЕІ основаны на «треугольном распределении».

Столбец первоначальных капиталовложений содержит суммы затрат, понесенные в «момент 0», то есть в начале первого года. Эти затраты не дисконтируются. Все остальные денежные потоки дисконтируются с помощью дисконтной ставки на конец года. Текущая стоимость (PV) вычисляется для каждой оценки суммы затрат и выгод. Чистая текущая выгода (NPV) в сводных таблицах представляет собой сумму начального капиталовложения и дисконтированных денежных потоков за каждый год. Из-за погрешности округления суммы по таблицам общей выгоды, общих затрат и денежных потоков могут незначительно отличаться от итоговых значений.



Текущая стоимость (PV)

Текущая выгода или выгода на данный момент дисконтированных затрат и выгод, оцениваемая на основании определенной процентной ставки (дисконтной ставки). Текущая стоимость затрат и выгод являются исходными величинами для вычисления суммарной чистой текущей стоимости денежных потоков.



Чистая текущая стоимость (NPV)

Текущая выгода или выгода на данный момент дисконтированных будущих чистых денежных потоков на основании определенной процентной ставки (дисконтной ставки). Положительная оценка NPV проекта обычно указывает на целесообразность данного капиталовложения, за исключением случаев, когда существуют альтернативные проекты с более высоким значением NPV.



Рентабельность инвестиций (ROI)

Ожидаемая доходность проекта, в процентах. Окупаемость инвестиций вычисляется делением чистой выгоды (выгоды за вычетом затрат) на затраты.



Дисконтная ставка

Процент, используемый в анализе потока денежных средств для учета изменения ценности денег с течением времени. В различных организациях дисконтная ставка может составлять от 8 до 16 %.



Срок окупаемости

Точка безубыточности капиталовложения. Момент времени, когда чистая выгода (выгода за вычетом затрат) равна начальным капиталовложениям или затратам.

Приложение Б. Примечания

¹ Источник: «Защита промышленных систем управления и ключевой инфраструктуры от атак» (Protecting Industrial Control Systems And Critical Infrastructure From Attack), исследование Forrester Research, Inc., 19 апреля 2018 г.

² Источник: «Исследование стоимости киберпреступности» (Cost Of Cyber Crime Study), Ponemon Institute, 2017 г.
(<https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017>).

³ Источник: Там же.

⁴ Источник: «Защита промышленных систем управления и ключевой инфраструктуры от атак» (Protecting Industrial Control Systems And Critical Infrastructure From Attack), исследование Forrester Research, Inc., 19 апреля 2018 г.