Реализация требований 187-ФЗ с использованием решений АО «Лаборатория Касперского»

27.04.2021
г.Москва

kaspersky



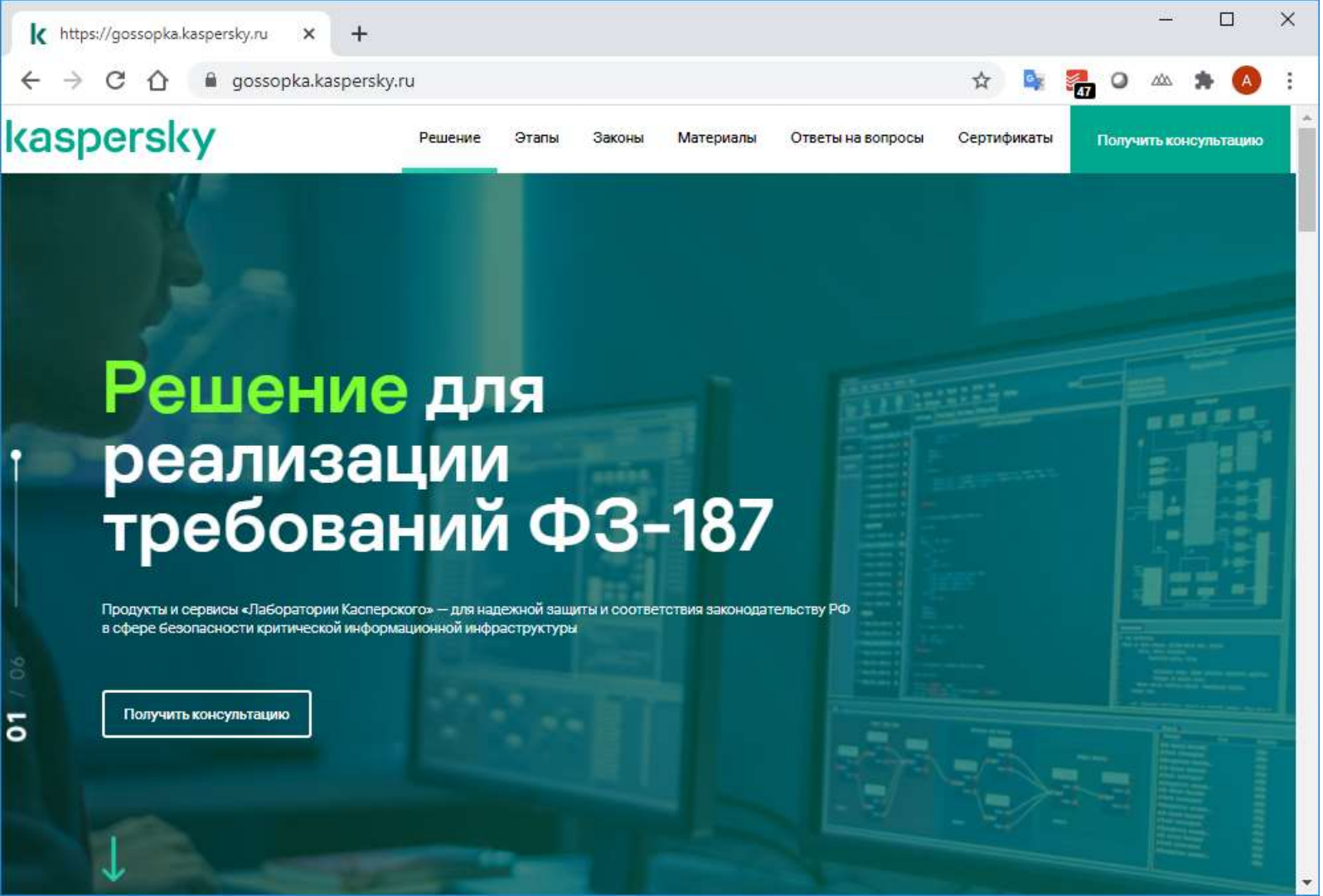
Киселев Алексей
Менеджер по развитию бизнеса
alexey.kiselev@kaspersky.com
Тел: +7 495 797 87 00 (774877)
gossopka.kaspersky.ru

kaspersky

Обновление сайта: gossopka.kaspersky.ru

- Описание этапов реализации требований 187-ФЗ
- Нормативная база
- Карта решений

kaspersky


https://gossopka.kaspersky.ru
gossopka.kaspersky.ru
kaspersky
Решение
Этапы
Законы
Материалы
Ответы на вопросы
Сертификаты
Получить консультацию
Решение для реализации требований ФЗ-187
Продукты и сервисы «Лаборатории Касперского» — для надежной защиты и соответствия законодательству РФ в сфере безопасности критической информационной инфраструктуры
Получить консультацию
01 / 06

Этапы реализации

Реализация требований законодательства РФ проходит в несколько этапов. Наши решения помогут организациям соответствовать требованиям законодательства РФ в области безопасности КИИ, в том числе к построению центров ГосСОПКА. Подробнее о действиях по реализации нормативных требований читайте на странице Этапы реализации.

1

Первичный сбор данных

На начальном этапе организация определяет, является ли она субъектом КИИ. Для этого она готовит перечни ИС, АСУ, ИТС и определяет сферы функционирования каждой из них.

Результат этой работы — вывод о необходимости (или отсутствии необходимости) выполнения организацией требований 187-ФЗ.

2

Проведение категорирования

Организация создает комиссию по категорированию, определяет объекты категорирования, а затем определяет категории значимости для объектов КИИ.

После этого она согласует со ФСТЭК России перечень объектов КИИ с присвоенными (либо не присвоенными) категориями значимости.

Подробнее

3

Нет значимых объектов КИИ

Организация должна обеспечить соответствие 9 статьи ФЗ-187 (часть 2), в частности незамедлительно информировать о компьютерных инцидентах федеральные органы исполнительной власти.

Подробнее

3

Есть значимые объекты КИИ

Организация должна:

- Разработать план реагирования на компьютерные инциденты
- Создать систему безопасности значимых объектов КИИ в соответствии с приказами ФСТЭК №235 и №239
- Выбрать способ реализации функций ГосСОПКА.

Подробнее

Для всех субъектов КИИ

Для субъектов КИИ, имеющих значимые объекты КИИ

Для субъектов КИИ, не имеющих значимые объекты КИИ

Разработка мероприятий по взаимодействию со ФСБ России.

В том числе это относится к организациям, у которых нет значимых объектов КИИ, так как организация должна обеспечить соответствие 9 статьи ФЗ-187 (часть 2), в частности незамедлительно информировать о компьютерных инцидентах федеральные органы исполнительной власти.

Проводимые работы

1. Разработать и утвердить регламент информирования НКЦКИ об инцидентах.
2. Реализовать подключение к технической инфраструктуре НКЦКИ (при выборе данного способа информирования).

Решения «Лаборатории Касперского»

SIEM-система Kaspersky Unified Monitoring & Analysis Platform, подключенная к технической инфраструктуре НКЦКИ для автоматизированного взаимодействия в соответствии с требованиями 187-ФЗ, приказами ФСБ РФ №367, №368[1] (при выборе данного способа информирования).

Результаты

1. Утвержденный регламент информирования НКЦКИ об инцидентах.
2. Внедренное средство мониторинга и реагирования на инциденты, интегрированное с технической инфраструктурой НКЦКИ.

---

[1] Функциональность KUMA по подключению к технической инфраструктуре НКЦКИ выйдет в официальном релизе в 2021 году.

- Для всех субъектов КИИ
- **Для субъектов КИИ, имеющих значимые объекты КИИ**
- Для субъектов КИИ, не имеющих значимые объекты КИИ

Разработка плана реагирования на компьютерные инциденты (КИ) и принятия мер по ликвидации последствий компьютерных атак (КА) в соответствии с требованиями приказа ФСБ России №282.

Создание системы безопасности значимых объектов КИИ в соответствии с требованиями приказов ФСТЭК России №235, 239.

Выбор способа реализации функций субъекта ГосСОПКА



Для субъектов КИИ, имеющих значимые объекты КИИ



Для субъектов КИИ, не имеющих значимые объекты КИИ

Создание системы безопасности значимых объектов КИИ в соответствии с требованиями приказов ФСТЭК России №235, 239.

Проводимые работы

1. Установить требования.
2. Разработать организационные и технические меры.
3. Внедрить организационные и технические меры.

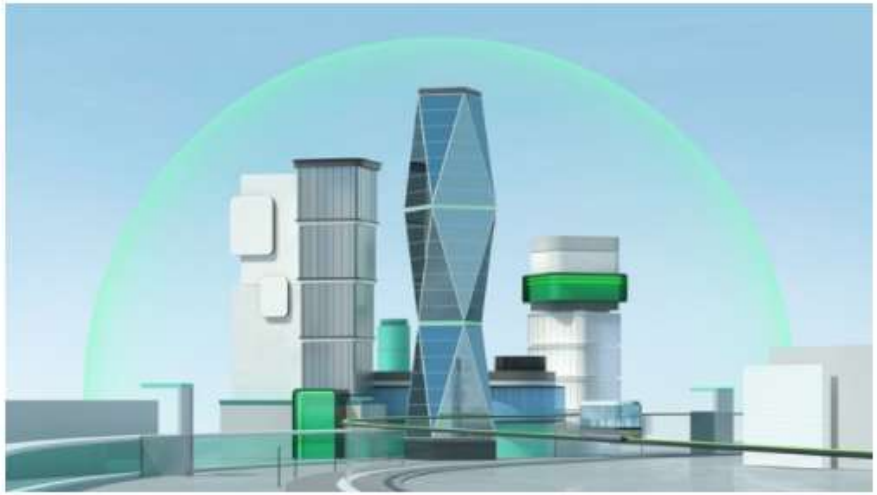
Решения «Лаборатории Касперского»

- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Security Center
- Kaspersky Security для бизнеса
- Kaspersky Web Traffic Security
- Kaspersky Secure Mail Gateway
- Kaspersky Endpoint Detection and Response
- Kaspersky Anti Targeted Attack
- Kaspersky Security для систем хранения данных
- Kaspersky Sandbox
- Kaspersky Security Awareness

Реализация требований приказа ФСТЭК России №239 с помощью решений «Лаборатории Касперского»

О соответствии мер, указанных в приказе, функциональности продуктов и сервисов «Лаборатории Касперского».

Скачать



Обозначение и номер меры	Меры обеспечения безопасности значимого объекта КИИ	3	2	1	Закрывает Да / Нет / Частично	Способ реализации, наименование решения «Лаборатории Касперского»	Функции, реализуемые решениями ЛК
I. Идентификация и аутентификация (ИАФ)							
ИАФ.2	Идентификация и аутентификация устройств				Частично	Kaspersky Endpoint Security	Контроль устройств: позволяет создавать политики подключение съемных носителей и других периферийных устройств; осуществлять контроль доступа программ.
					Частично	KICS For Nods	
					Частично	KICS For Networks	Network Integrity Control: позволяет идентифицировать все сетевые ресурсы, подключенные к Ethernet – включая SCADA-серверы, HMI, инженерные рабочие станции, PLCs, IEDs и RTU.
III. Ограничение программной среды (ОПС)							
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения			+	Частично	Kaspersky Endpoint Security	Контроль программ: позволяет разрешать, блокировать и регулировать использование программ.
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения		+	+	Частично	Kaspersky Security Center	Systems Management: позволяет автоматизировать для Windows-устройств задачи установки ПО и патч-менеджмента.
IV. Защита машинных носителей информации (ЗНИ)							
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации	+	+	+	Частично	Kaspersky Endpoint Security	Контроль устройств: позволяет создавать политики подключения съемных носителей и контролировать операции записи и удаления файлов на них.
ЗНИ.7	Контроль подключения съемных машинных носителей информации	+	+	+	Частично	Kaspersky Endpoint Security	Контроль устройств: позволяет создавать политики подключения съемных носителей и других периферийных устройств.
V. Аудит безопасности (АУД)							
АУД.1	Инвентаризация информационных ресурсов	+	+	+	Частично	Kaspersky Security Center, Kaspersky Systems Management, KICS for Networks	Позволяет реализовать инвентаризацию информационных ресурсов в корпоративной сети для Windows-устройств (Kaspersky Security Center) и сетях АСУ ТП (KICS).
						Kaspersky Security Center Kaspersky	Kaspersky Security Center позволяет обнаружить

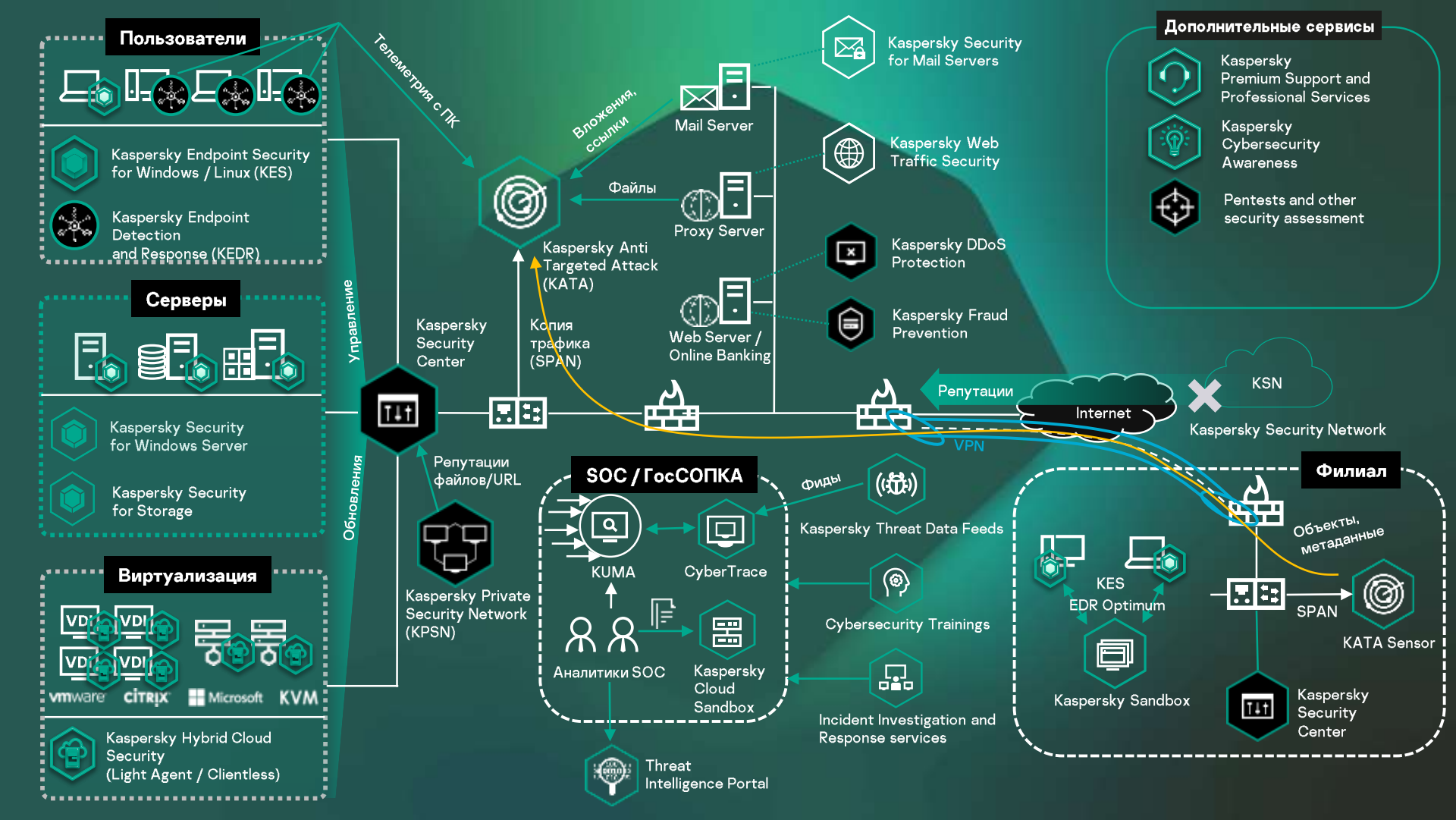
АУД.4	Регистрация событий безопасности	+	+	+	Частично	Kaspersky Unified Monitoring and Analysis Platform	Позволяет регистрировать события безопасности поступающие от любых источников
						Kaspersky Security Center	Позволяет регистрировать события безопасности поступающие от средств защиты Лаборатории Касперского
АУД.5	Контроль и анализ сетевого трафика			+	Да	Kaspersky Anti Targeted Attack, KICS for Networks	Решения «Лаборатории Касперского» позволяют осуществлять сбор и анализ событий безопасности сетевого трафика в корпоративных (Kaspersky Anti Targeted Attack) и промышленных (KICS for Networks) сетях.
АУД.6	Защита информации о событиях безопасности	+	+	+	Да	Kaspersky Unified Monitoring and Analysis Platform / Kaspersky Security Center (SMC)	
АУД.7	Мониторинг безопасности	+	+	+	Да	Kaspersky Unified Monitoring and Analysis Platform	Позволяет централизованно осуществлять мониторинг событий безопаности, поступающих от любых источников информации защищаемой инфраструктуры.
						Kaspersky Endpoint Detection and Response	Позволяет осуществлять автоматизированный мониторинг безопасности рабочих станций под управлением Windows и Linux.
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	+	+	Да	Kaspersky Endpoint Detection and Response	Позволяет централизованно и автоматизированно осуществлять реагирование на инциденты безопасноти, связанные с защищаемыми рабочими станциями. Например изолировать компьютер от сети, получить подозрительный файл, остановить подозрительный процесс и т. д.
						Kaspersky Incident Response	Профессиональная команда экспертов поможет сдержать распространение заражения, установить причины и устранить последствия инцидента.
АУД.9	Анализ действий отдельных пользователей			+	Частично	Kaspersky Endpoint Detection and Response	Kaspersky Endpoint Detection and Response позволят собирать, хранить и автомтизированно обрабатывать информацию о сетевых сессиях, активности процессов, изменениях системы на рабочих станциях пользователей.
АУД.10	Проведение внутренних аудитов	+	+	+	Да		
АУД.11	Проведение внешних аудитов				Да	Сервисы анализа защищенности	Проведение тестирования на проникновение, анализа защищенности приложений, обнаружения текущей активности вредоносного ПО в сети (Targeted Attack Discovery), анализ защищенности промышленных сиситем.
VI. Антивирусная защита (АВЗ)							

АВ3.1	Реализация антивирусной защиты	+	+	+	Да	Security,KSV,Kaspersky Secure Mail Gateway,Kaspersky Web Traffic Security, ScanEngine, KICS for Nodes	защиту корпоративной сети от известных, неизвестных и сложных угроз. Сочетает аналитические данные, технологии машинного обучения и опыт экспертов.
АВ3.2	Антивирусная защита электронной почты и иных сервисов	+	+	+	Да	Kaspersky Secure Mail Gateway, Kaspersky Web Traffic Security, Kaspersky Scan Engine (KSE)	Позволяют осуществить антивирусную защиту почтовых серверов (Kaspersky Secure Mail Gateway), интернет-шлюзов (Kaspersky Web Traffic Security) и любых других бизнес-сервисов (KSE).
АВ3.3	Контроль использования архивных, исполняемых и зашифрованных файлов			+	Да	Kaspersky Endpoint Security,KSV,Kaspersky Secure Mail Gateway,Kaspersky Web Traffic Security, ScanEngine, KICS for Nodes	С помощью политик можно настроить обработку запароллених архивов, глубину сканирования и т. д.
АВ3.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	Да	штатный функционал всех решений «Лаборатории Касперского», KPSN	Регулярное, в том числе автоматическое обновление баз данных антивирусных программ, а также облачная база знаний KSN (в том числе приватная - KPSN).
АВ3.5	Использование средств антивирусной защиты различных производителей			+	Частично	Kaspersky Security Center,Kaspersky Endpoint Security,KSV,Kaspersky Secure Mail Gateway,Kaspersky Web Traffic Security, ScanEngine, KICS for Nodes	Дополнительно необходимо добавить средства антивирусной защиты других прозводителей.
VII. Предотвращение вторжений (компьютерных атак) (СОВ)							
СОВ.1	Обнаружение и предотвращение компьютерных атак		+	+	Да	Kaspersky Anti Targeted Attack + Kaspersky Endpoint Detection and Response, KICS for Networks, Kaspersky Unified Monitoring and Analysis Platform	Сбор событий безопасности сетевого трафика (Kaspersky Anti Targeted Attack), рабочих станций (Kaspersky Endpoint Detection and Response), промышленных сетей (KICS). Анализ событий безопасности, их корреляция и оценка уровня риска (Kaspersky Unified Monitoring and Analysis Platform).

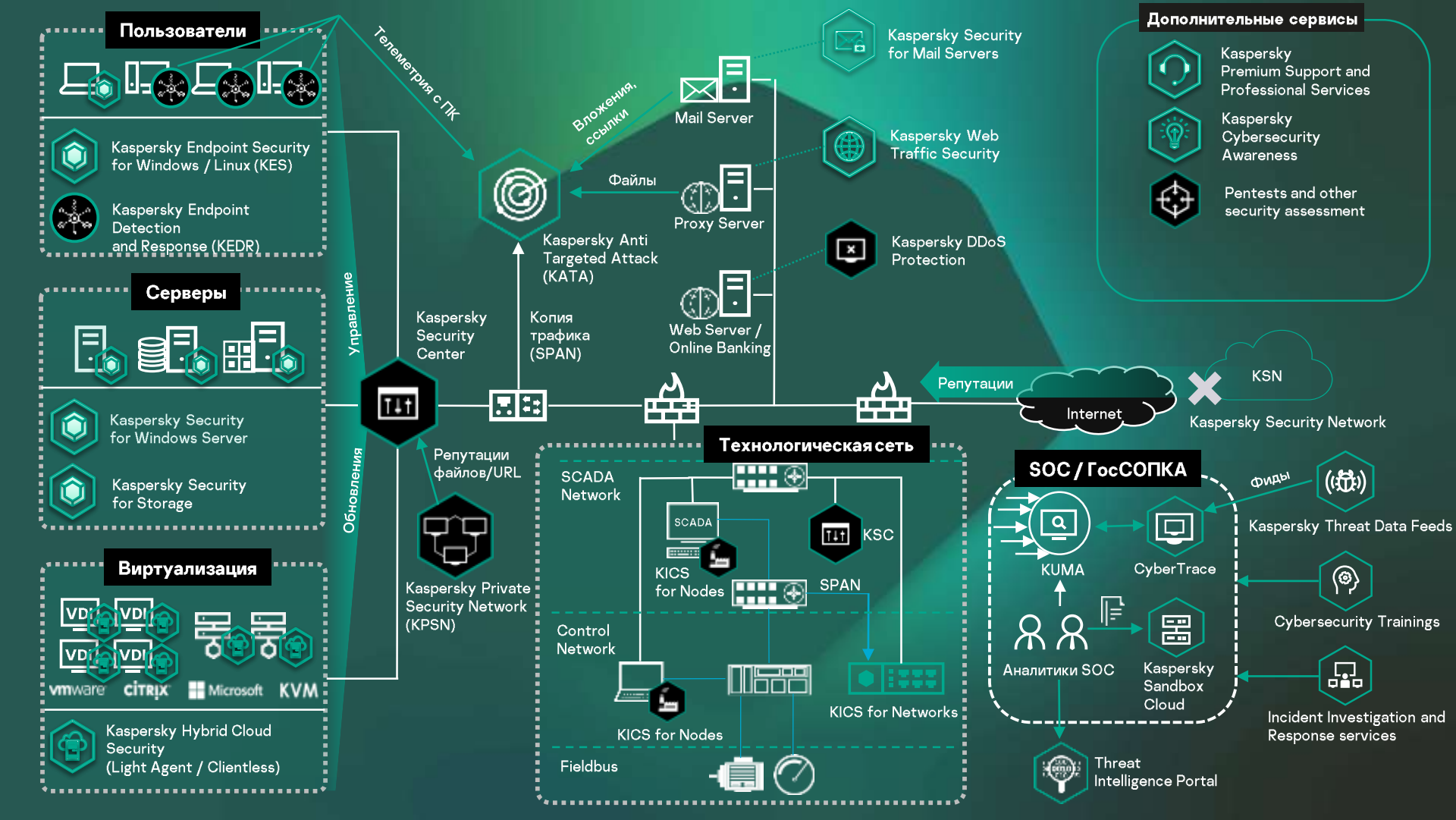
ОЦЛ.1	Контроль целостности программного обеспечения	+	+	+	Частично	для виртуальных и облачных сред Enterprise, KICS for Nodes	контроль целостности объектов системы путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы.
ОЦЛ.2	Контроль целостности информации				Частично	Kaspersky Security для виртуальных и облачных сред Enterprise (FIM), KICS for Nodes	
IX. Обеспечение доступности (ОДТ)							
ОДТ.3	Контроль безотказного функционирования средств и систем		+	+	Частично	Kaspersky DDoS Protection	Решение позволяет выявлять и защищать ИС от атак типа отказ в обслуживании.
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)							
ЗИС.2	Защита периметра информационной (автоматизированной) системы	+	+	+	Частично	Kaspersky Web Traffic Security	Позволят обеспечить защиту и контроль доступа пользователей в интернет.
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	+	+	+	Да		Весь комплекс решений «Лаборатории Касперского» для защиты информационных систем на различных уровнях.
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения ("песочница")				Да	Kaspersky Anti Targeted Attack, Kaspersky Sandbox, Cloud Sandbox, Research Sandbox	Позволяют сканировать подозрительные объекты в изолированной среде с вынесением соответствующего вердикта.
ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти				Нет		
ЗИС.13	Защита неизменяемых данных		+	+	Частично	Kaspersky Security для виртуальных и облачных сред Enterprise KICS for Nodes	Модуль File Integrity Monitor позвоялет осуществлять контроль целостности объектов системы путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы.
ЗИС.15	Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек				Да	Kaspersky Secure Mail Gateway	Kaspersky Secure Mail Gateway позволяет организовать контроль за используемыми в организации точками электронного почтового обмена
ЗИС.16	Защита от спама		+	+	Да	Kaspersky Secure Mail Gateway	Защита почтовых серверов от спам-рассылок.
	Блокировка доступа к сайтам или типам сайтов					Kaspersky Web Traffic	Kaspersky Web Traffic Security позволяет организовать централизованный котнроль доступа в интернет.

ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+	+	+	Да	Kaspersky Endpoint Security (Контроль устройств)	Контроль устройств управляет доступом пользователей к установленным или подключенным к компьютеру переферийным устройствам (например, жестким дискам, камере или модулю Wi-Fi). Это позволяет защитить компьютер от заражения при подключении этих устройств и предотвратить потерю или утечку данных.
ЗИС.23	Контроль использования мобильного кода				Частично	Kaspersky Endpoint Security (Адаптивный контроль аномалий+AMSI), Kaspersky Endpoint Detection and Response	Модули адптивный контроль аномалий и AMSI защита позволяют обеспечивать Kaspersky Endpoint Security контроль и антивирусная проверку используемых скриптов. Использование Kaspersky Endpoint Detection and Response позволит обеспечить более продвинутый уровень защиты, возможность настроить свои правила детектирования, а также упростит процесс раследования связанных инцидентов.
ЗИС.31	Защита от скрытых каналов передачи информации				Частично	Kaspersky Anti Targeted Attack	Решение имеет инструменты для выявления аномальной сетевой активности, в том числе с использованием техник скорытия передачи информации
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOSНетатак)	+	+	+	Да	Kaspersky DDoS Protection	Обеспечивает защиту от DDoS-атак до L7 уровня модели OSI.
ЗИС.35	Управление сетевыми соединениями	+	+	+	Частично	Kaspersky Endpoint Security (Межсетевой экран)	Встроенный в Kaspersky Endpoint Security межсетевой экран позволяет управлять сетевыми соединениями на защищемых рабочих станциях.
ЗИС.38	Защита информации при использовании мобильных устройств	+	+	+	Да	Kaspersky Endpoint Security for Android, Kaspersky Endpoint Security for Aurora	Использование Kaspersky Endpoint Security for Android с централизованным управлением через Kaspersky Security Center позволяет защищать мобильные устройства на базе соответсвующей ОС. Также в нашем портфолио есть специализированное защитное решение для отечественной мобильной платформы Аврора.
XII. Реагирование на компьютерные инциденты (ИНЦ)							
ИНЦ.1	Выявление компьютерных инцидентов	+	+	+	Да	Kaspersky Unified Monitoring and Analysis Platform, Kaspersky Anti Targeted Attack, Kaspersky Endpoint Detection and Response	Позволяют выявлять компьютерные инциденты на основании поступающих данных. Kaspersky Anti Targeted Attack - сетевой и почтовый трафик Kaspersky Endpoint Detection and Response - события на конечном узле с установленым агентом Kaspersky Unified Monitoring and Analysis Platform - на основании правил корреляции событий от подключенных источников

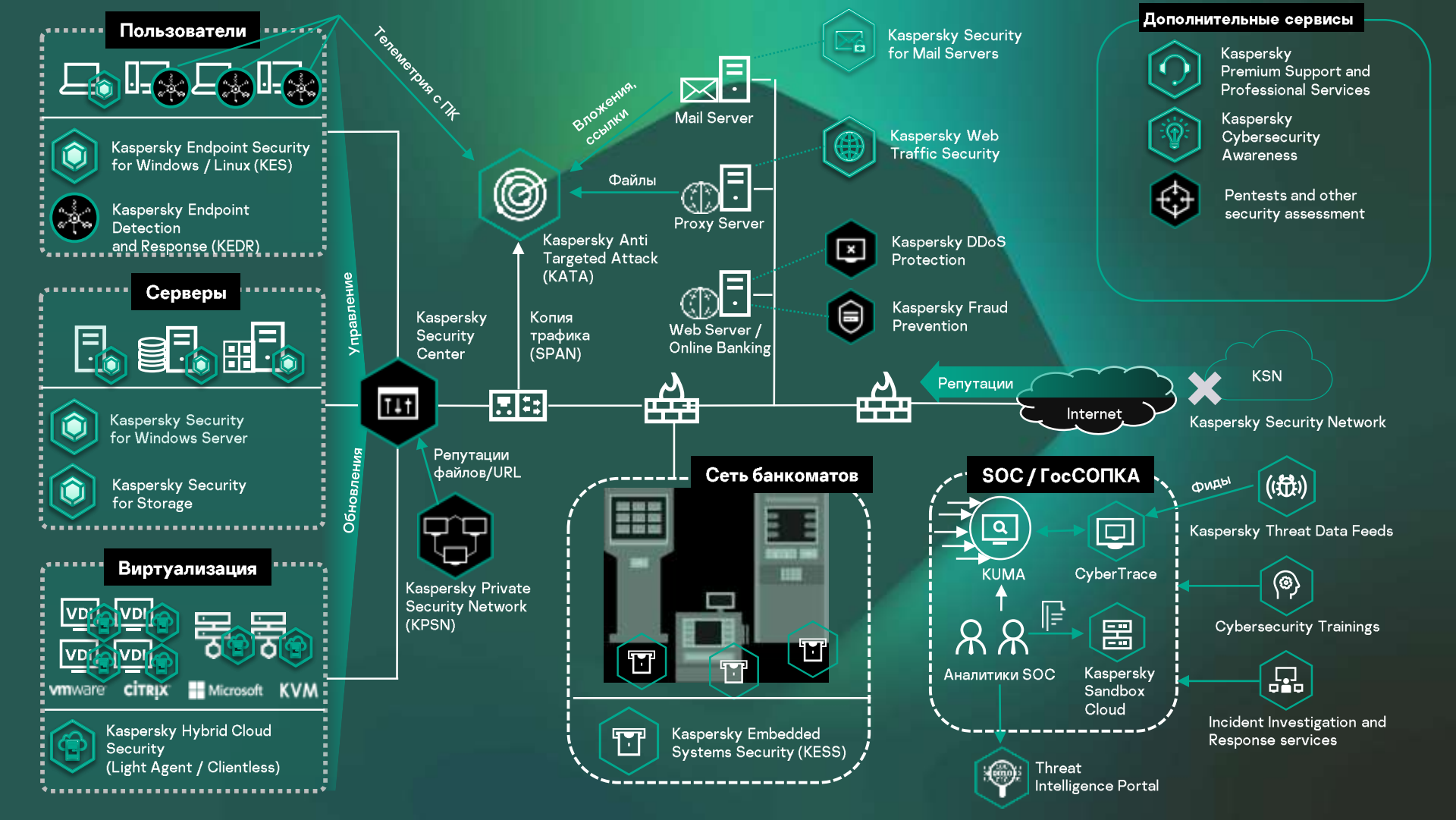
Типовое предприятие


Пользователи
Kaspersky Endpoint Security for Windows / Linux (KES)
Kaspersky Endpoint Detection and Response (KEDR)
Серверы
Kaspersky Security for Windows Server
Kaspersky Security for Storage
Виртуализация
VDI
vmware
CITRIX
Microsoft
KVM
Kaspersky Hybrid Cloud Security (Light Agent / Clientless)
Телеметрия с ПК
Управление
Обновления
Вложения, ссылки
Файлы
Mail Server
Proxy Server
Web Server / Online Banking
Kaspersky Anti Targeted Attack (KATA)
Копия трафика (SPAN)
Kaspersky Security Center
Репутации файлов/URL
Kaspersky Private Security Network (KPSN)
Kaspersky Security for Mail Servers
Kaspersky Web Traffic Security
Kaspersky DDoS Protection
Kaspersky Fraud Prevention
Репутации
Internet
KSN
Kaspersky Security Network
VPN
Дополнительные сервисы
Kaspersky Premium Support and Professional Services
Kaspersky Cybersecurity Awareness
Pentests and other security assessment
SOC / ГосСОПКА
KUMA
CyberTrace
Аналитики SOC
Kaspersky Cloud Sandbox
Threat Intelligence Portal
Фиды
Kaspersky Threat Data Feeds
Cybersecurity Trainings
Incident Investigation and Response services
Филиал
KES
EDR Optimum
Kaspersky Sandbox
Объекты, метаданные
SPAN
KATA Sensor
Kaspersky Security Center

Типовое промышленное предприятие


Пользователи
Kaspersky Endpoint Security for Windows / Linux (KES)
Kaspersky Endpoint Detection and Response (KEDR)
Серверы
Kaspersky Security for Windows Server
Kaspersky Security for Storage
Виртуализация
Kaspersky Hybrid Cloud Security (Light Agent / Clientless)
Телеметрия с ПК
Управление
Обновления
Вложения, ссылки
Файлы
Копия трафика (SPAN)
Kaspersky Anti Targeted Attack (KATA)
Kaspersky Security Center
Репутации файлов/URL
Kaspersky Private Security Network (KPSN)
Mail Server
Proxy Server
Web Server / Online Banking
Kaspersky Security for Mail Servers
Kaspersky Web Traffic Security
Kaspersky DDoS Protection
Дополнительные сервисы
Kaspersky Premium Support and Professional Services
Kaspersky Cybersecurity Awareness
Pentests and other security assessment
Репутации
Internet
KSN
Kaspersky Security Network
Технологическая сеть
SCADA Network
SCADA
KSC
KICS for Nodes
SPAN
Control Network
KICS for Networks
KICS for Nodes
Fieldbus
SOC / ГосСОПКА
Фиды
Kaspersky Threat Data Feeds
KUMA
CyberTrace
Cybersecurity Trainings
Аналитики SOC
Kaspersky Sandbox Cloud
Incident Investigation and Response services
Threat Intelligence Portal

Типовое финансовое предприятие


Пользователи
Kaspersky Endpoint Security for Windows / Linux (KES)
Kaspersky Endpoint Detection and Response (KEDR)
Серверы
Kaspersky Security for Windows Server
Kaspersky Security for Storage
Виртуализация
Kaspersky Hybrid Cloud Security (Light Agent / Clientless)
Телеметрия с ПК
Управление
Обновления
Вложения, ссылки
Файлы
Mail Server
Proxy Server
Web Server / Online Banking
Kaspersky Anti Targeted Attack (KATA)
Копия трафика (SPAN)
Kaspersky Security Center
Репутации файлов/URL
Kaspersky Private Security Network (KPSN)
Kaspersky Security for Mail Servers
Kaspersky Web Traffic Security
Kaspersky DDoS Protection
Kaspersky Fraud Prevention
Дополнительные сервисы
Kaspersky Premium Support and Professional Services
Kaspersky Cybersecurity Awareness
Pentests and other security assessment
Репутации
Internet
KSN
Kaspersky Security Network
Сеть банкоматов
Kaspersky Embedded Systems Security (KESS)
SOC / ГосСОПКА
KUMA
CyberTrace
Аналитики SOC
Kaspersky Sandbox Cloud
Threat Intelligence Portal
Фиды
Kaspersky Threat Data Feeds
Cybersecurity Trainings
Incident Investigation and Response services

Спасибо за внимание!

Киселев Алексей Анатольевич
Office: +7 495 797 87 00 x4877
alexey.kiselev@kaspersky.com

АО "Лаборатория Касперского"
Москва, 125212
Ленинградское шоссе, д.39А, стр.3
+7 (495) 797-87-00
www.kaspersky.ru

kaspersky