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

kaspersky

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).
АУД.2	Анализ уязвимостей и их устранение	+	+	+	Частично	Kaspersky Security Center Kaspersky Systems Management	Kaspersky Security Center позволяет обнаружить и закрыть уязвимости в операционных системах и программах сторонних производителей на устройствах под управлением Windows.
						KICS for Networks	KICS for Networks, начиная с версии 3.0, позволит осуществлять пассивный поиск уязвимостей на вывленнных устройствах сети АСУ ТП.

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	Kaspersky Security Center,Kaspersky Endpoint Security,KSV,Kaspersky Secure Mail Gateway,Kaspersky Web Traffic Security, ScanEngine, KICS for Nodes	Позволяют осуществить комплексную многоуровневую 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).
СОВ.2	Обновление базы решающих правил		+	+	Да	штатный функционал всех решений Лаборатории Касперского, KPSN	Регулярное обновление правил IDS и индикаторов атак (IoA)

VIII. Обеспечение целостности (ОЦЛ)							
ОЦЛ.1	Контроль целостности программного обеспечения	+	+	+	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.
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.
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию				Да	Kaspersky Web Traffic Security, Kaspersky Endpoint Security	Kaspersky Web Traffic Security позволяет организовать централизованный котнроль доступа в интернет. Так же с помощью модуля Веб-контроль на Kaspersky Endpoint Security возможножного реализацовать политики 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 расследования 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

ИНЦ.2	Информирование о компьютерных инцидентах	+	+	+	Да	Kaspersky Unified Monitoring and Analysis Platform, Kaspersky Anti Targeted Attack, Kaspersky Endpoint Detection and Response	Kaspersky Anti Targeted Attack и Kaspersky Endpoint Detection and Response: позволяют просматривать инциденты в вею-консоли, отправлять уведомления на электронную почту и отправлять события в SIEM. Kaspersky Unified Monitoring and Analysis Platform - Позволяет просматривать инциденты в WEB-консоли, отправлять уведомления на почту и настроить интерграцию со сторонней системой.
ИНЦ.3	Анализ компьютерных инцидентов	+	+	+	Да	Kaspersky Unified Monitoring and Analysis Platform, Kaspersky Anti Targeted Attack, Kaspersky Endpoint Detection and Response	Kaspersky Anti Targeted Attack и Kaspersky Endpoint Detection and Response: позволяют проводить анализ компьютерных инцидентов предоставляя в карточке инцидента подробную информацию. Kaspersky Unified Monitoring and Analysis Platform: позволяет проводить анализ компютерных инцидентов в карточке инцидента на основании поступивших событий и правил корреляции.
ИНЦ.4	Устранение последствий компьютерных инцидентов	+	+	+	Да	Kaspersky Endpoint Detection and Response	Предоставляет возможности реагирования на инцидент, используя компонент Endpoint Sensors: • Блокировка запуска ПО / скриптов / документов • Завершение процесса • Удаление файла • Получение файл с конечного узла в хранилище • Карантин файла / восстановление из карантина • Запуск программы • Выполнение IoC-сканирования на конечных узлах, а также по базе собранных событий • Выполнение сетевой изоляции конечных устройств
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	+	+	+	Частично	Kaspersky Endpoint Detection and Response	Предоставляет возможности реагирования на инцидент, используя компонент Endpoint Sensors: • Блокировка запуска ПО / скриптов / документов • Завершение процесса • Удаление файла • Получение файл с конечного узла в хранилище • Карантин файла / восстановление из карантина • Запуск программы • Выполнение IoC-сканирования на конечных узлах, а также по базе собранных событий • Выполнение сетевой изоляции конечных устройств
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	+	+	+	Да	Kaspersky Unified Monitoring and Analysis Platform,Kaspersky Anti Targeted Attack,Kaspersky Endpoint Detection and Response	Kaspersky Anti Targeted Attack, Kaspersky Endpoint Detection and Response и Kaspersky Unified Monitoring and Analysis Platform позволяют хранить информацию о компьюретных инцидентах в собственных базад данных, обеспечивая при этом невозможность просмотра инцидентов неуполномоченным сотрудникам.
XIII. Управление конфигурацией (УКФ)							
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+	+	+	Да	Kaspersky Endpoint Security	Контроль программ: позволяет разрешать, блокировать и регулировать использование программ, в т. ч. ведение «белого списка» разрешенных программ.

XIV. Управление обновлениями программного обеспечения (ОПО)							
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	+	+	+	Частично	Kaspersky Security Center	Systems Management: позволяет для Windows-устройств автоматизировать задачи установки ПО, патч-менеджмента.
ОПО.3	Тестирование обновлений программного обеспечения	+	+	+	Частично	Kaspersky Sandbox, Cloud Sandbox, Research Sandbox	Позволяют сканировать объекты (в т. ч. после процедуры обновления) в изолированной среде с вынесением соответствующего вердикта.
ОПО.4	Установка обновлений программного обеспечения	+	+	+	Частично	Kaspersky Security Center	Kaspersky Systems Management: позволяет для Windows-устройств автоматизировать задачи установки ПО, патч-менеджмента.
XVI. Обеспечение действий в нештатных ситуациях (ДНС)							
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	+	+	+	Частично	Kaspersky Cybersecurity Trainings	Обучение по курсам: - Реагирование на инциденты - Анализ вредоносного ПО - Цифровая криминалистика - Эффективное обнаружение угроз с помощью YARA
XVII. Информирование и обучение персонала (ИПО)							
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	+	+	+	Да	Kaspersky Automated Security Awareness Platform	Позволяет оценить текущие знания сотрудника в сфере кибербезопасности, определить в соответствии с этим набор навыков, необходимых именно ему, выстроить график прохождения программы и осуществить контроль усвоения материала.
ИПО.2	Обучение персонала правилам безопасной работы	+	+	+	Да	Kaspersky Automated Security Awareness Platform	
ИПО.3	Проведение практических занятий с персоналом по правилам безопасной работы		+	+	Да	Kaspersky Automated Security Awareness Platform	
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	+	+	+	Да	Kaspersky Automated Security Awareness Platform	

Примечание

Настоящая таблица носит информационный характер и не была согласована с регулирующими органами.
Не вся функциональность заявленных продуктов была сертифицирована.

По всем вопросам обращайтесь к представителю «Лаборатории Касперского», оставив заявку на сайте **gossopka.kaspersky.ru**.

www.kaspersky.ru

kaspersky **АКТИВИРУЙ БУДУЩЕЕ**

© 2021 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.