????????

Приказ ФСТЭК России № 239 является ключевым нормативным документом, который регулирует вопросы обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры (далее – КИИ) Российской Федерации.

Приказ № 239 направлен на достижение ряда важных целей в области обеспечения информационной безопасности:

- Обеспечение национальной безопасности и устойчивости объектов КИИ

Объекты КИИ представляют собой информационные системы, сети и автоматизированные системы управления критически важных предприятий, поэтому нарушение работы данных систем может нанести ущерб здоровью граждан, экономике, общественному порядку и безопасности государства. Приказ устанавливает требования, которые направленны на защиту перечисленных систем от компьютерных атак.

- Выполнение требований Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Приказ разработан в соответствии с требованиями Федерального закона № 187-ФЗ и является обязательным для всех субъектов КИИ, чьи объекты признаны значимыми.

- Внедрение Системы безопасности

В приказе предусмотрены 17 организационных и технических мер безопасности, которые помогают выстроить комплексную систему безопасности в организации, пример мер представлен ниже:

- Идентификацию и аутентификацию (ИАФ).
- Управление доступом (УПД).
- Аудит безопасности (АУД).
- Антивирусную защиту (АВЗ).
- Предотвращение вторжений (СОВ).
- Обеспечение целостности и доступности (ОЦЛ, ОДТ).
- Реагирование на инциденты (ИНЦ) и другие.

Нужно учитывать, что те или иные меры применяются в зависимости от категории значимости объекта КИИ, что позволяет гибко выстраивать

комплексную систему безопасности.

- Повышение осведомленности и подготовки персонала

Приказ № 239 обязывает субъектов КИИ формировать процесс обучения и информирования сотрудников по вопросам безопасности, что способствует повышению киберграмотности и снижению рисков, связанных с человеческим фактором.

- Взаимодействие с государственными системами

Приказ № 239 обязывает осуществлять интеграцию с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

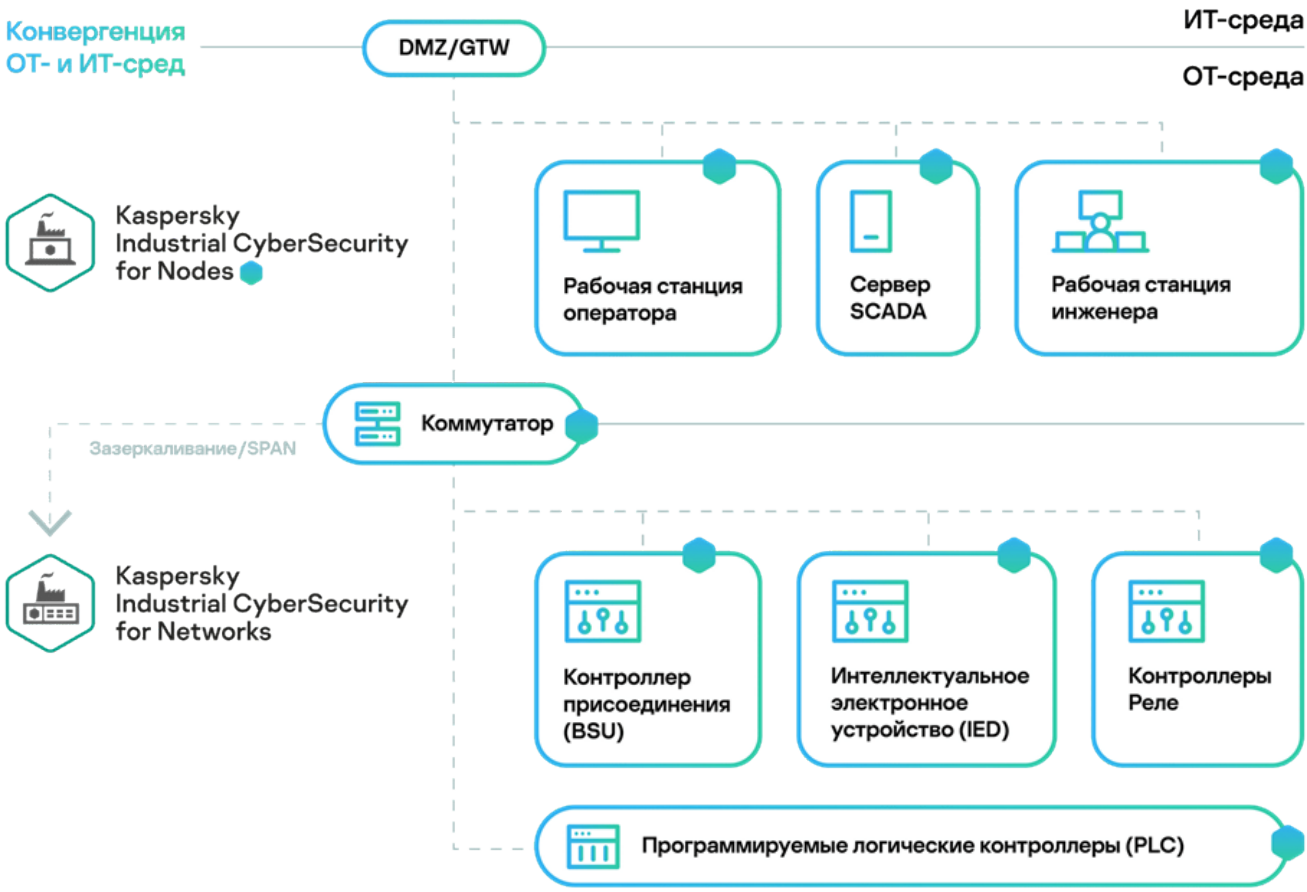
- Снижение рисков и минимизация последствий инцидентов.

Платформа Kaspersky Industrial CyberSecurity (далее - KICS) и решение класса SIEM - Kaspersky KUMA образуют мощный симбиоз для выполнения комплексных требований Приказа ФСТЭК России № 239.

KICS — это специализированная промышленная XDR-платформа, разработанная для комплексной защиты основных компонентов систем автоматизации и управления производством на всех уровнях, которая состоит из двух решений:

KICS for Nodes/ KICS for Linux Nodes со встроенной функциональностью EDR – решение, предназначенное для защиты рабочих мест, например, АРМ оператора, АРМ-инженера и т.д, также решение может осуществлять контроль целостности программ, исполняемых на ПЛК для управления технологическим процессом;

KICS for Networks – решение для защиты промышленных сетей, которое принимает копию трафика в одной или нескольких точках сети, а также телеметрию от узлов. На основании полученной телеметрии KICS for Networks изучает "нормальное" состояние сети, чтобы затем выявлять отклонения и аномалии. Помимо этого, KICS for Networks включает систему обнаружения вторжений (IDS), позволяет обнаруживать уязвимости устройств, небезопасную архитектуру сети, риски ИБ АСУ ТП, выполняет группировку и корреляцию своих событий и событий от KICS for Nodes. KICS for Networks предоставляет возможность активного опроса сети позволяет быстро и точно собирать данные о топологии сетей и настройках. Функция аудита рабочих мест помогает гарантировать соблюдение политик безопасности, включая безопасность текущих настроек, и организацию процесса выявления и митигации уязвимостей.



Kaspersky Security Center позволяет централизованно управлять программами KICS for Nodes и Kaspersky Endpoint Agent через политики и задачи, а также предоставляет интерфейс для анализа и реагирования на события безопасности от всех программ.

SIEM-система KUMA помогает усилить комплексную систему безопасности и собирает события от технологической, и от офисной сетей. Интегрируется с платформой KICS и позволяет централизованно управлять инцидентами.

Revision #8
Created 19 September 2025 10:55:13 by Olga Sinotova
Updated 23 September 2025 13:09:05 by Alexander Somonov