

Industrial CyberSecurity

В данной книге вы можете найти статьи, связанные с описание Industrial CyberSecurity и другое

- [Что такое Industrial CyberSecurity](#)
- [Kaspersky ICS EDR](#)
- [Особенности лицензирования платформы KICS](#)
- [В чем преимущество KICS for Nodes](#)

??? ????? Industrial CyberSecurity

????????

В настоящее время промышленные предприятия сталкиваются с растущими угрозами кибербезопасности. Эти угрозы могут привести к серьезным последствиям, таким как повреждение оборудования, остановка производства и утечка информации. Поэтому обеспечение безопасности промышленных систем становится одной из приоритетных задач для многих компаний.

Одной из основных проблем является интеграция безопасности в процессы проектирования и эксплуатации промышленных систем. Часто безопасность рассматривается как дополнение к основному функционалу, а не как неотъемлемая часть системы. Это приводит к тому, что меры безопасности принимаются уже после того, как система投入 в эксплуатацию, что значительно увеличивает затраты и снижает эффективность.

Важно отметить, что промышленная кибербезопасность (Industrial CyberSecurity) отличается от традиционной IT-безопасности. В то время как IT-безопасность фокусируется на защите информации, промышленная кибербезопасность охватывает защиту физических процессов, оборудования и инфраструктуры. Это требует комплексного подхода, включающего технические, организационные и человеческие факторы.

- Защита систем автоматического управления (SCADA),
- Защита программируемых логических контроллеров (PLC),
- Защита диспетчерских систем (DCS),
- Защита промышленных сетей (IIoT) и других критических элементов.

Для обеспечения безопасности промышленных систем необходимо внедрение комплексных мер, включающих регулярные обновления программного обеспечения, обучение персонала, проведение аудитов безопасности и создание резервных копий данных. Только такой подход позволит эффективно противостоять современным киберугрозам.

???????? Industrial CyberSecurity ?? IT-????????

Несмотря на общие принципы, защита промышленных систем существенно отличается от классической IT-безопасности.

В IT-среде основными приоритетами являются конфиденциальность и целостность данных. В ОТ-среде (Operational Technology) на первом месте стоит **доступность**: даже кратковременный простой может привести к серьёзным финансовым и технологическим потерям.

Ключевые отличия:

- промышленное оборудование часто работает десятилетиями и не поддерживает современные обновления безопасности;
- остановка системы для патча или перезагрузки может быть недопустима;
- многие промышленные протоколы изначально не проектировались с учётом киберугроз;
- ошибки в ОТ могут иметь физические последствия.

Поэтому методы защиты IT не всегда применимы напрямую в промышленности.

Индустриальная кибербезопасность: вызовы и решения

Индустриальная кибербезопасность (ICS/OT Security) — это область, посвящённая защите критической инфраструктуры от кибератак. В отличие от IT-среды, где данные являются основным активом, в ОТ-среде приоритетом является бесперебойная работа оборудования.

- Основные вызовы ИКБ в промышленности:
 1. Устаревшее оборудование: многие системы не имеют возможности обновлений.
 2. Отсутствие стандартизации: разрозненные протоколы и форматы данных.
 3. Высокие требования к доступности: даже минимальный простой может привести к значительным убыткам.
 4. Сложная архитектура: интеграция различных систем и устройств.
 5. Недостаток квалифицированных кадров: специалистов в области ИКБ в промышленности не хватает.
 6. Физические последствия: успешная атака может привести к повреждению оборудования или人身伤害.
 7. Отсутствие четкой ответственности: разделение обязанностей между IT и ОТ-отделами.
 8. Слабая осведомленность: сотрудники часто не осознают угрозы кибербезопасности.
 9. Ограниченные ресурсы: высокие затраты на внедрение и поддержку ИКБ.
 10. Отсутствие единой платформы: необходимость интеграции различных инструментов.
 11. Сложность мониторинга: огромный объем данных и событий.
 12. Недостаток информации: отсутствие полной картины угроз и инцидентов.
 13. Отсутствие тестирования: редкие учения и тестирование систем.
- Основные решения и стратегии:
 1. Внедрение сегментации сети: разделение OT-сети от IT-сети.
 2. Регулярное обновление ПО: установка патчей и обновление прошивок.
 3. Внедрение систем мониторинга: использование SIEM-систем и специализированных инструментов.
- Заключение:
 1. ИКБ в промышленности — это комплексная задача, требующая сотрудничества IT и ОТ-отделов.

1. ИКБ в промышленности;

2. ????????????????? ????? ????????????????? ??? ??;
3. ??????, ????????????????? ?? ????????? ??????.

??????? ????????????? ????????????????? ???????????????????? ????????????????? ?????????????????

??????? ????????????? ????????????????? ????????????????? ?? ?????????????????
???????????????? ?????????? ?? ????????????? ??????:

- Основные
- Фокусные
- Решения на базе KasperskyOS

??????????

1. Система комплексной защиты серверов и рабочих станций:
 1. Kaspersky Industrial CyberSecurity for Nodes (Linux&Windows)
2. Система ?????????????? ?????????? ? ????????????????????? ????? ??? ?
 1. Kaspersky Industrial CyberSecurity for Networks
3. Система мониторинга, анализа и управления событиями безопасности в промышленной инфраструктуре
 1. Kaspersky Unified Monitoring and Analysis Platform

??????????

1. Система раннего обнаружения аномалий с использованием машинного обучения
 1. Kaspersky Machine Learning for Anomaly Detection
2. Система построения программно-определяемых глобальных сетей
 1. Kaspersky SD-WAN
3. Система противодействия БПЛА
 1. Kaspersky Antidrone

????????? ?? ????? KasperskyOS

1. Тонкие клиенты
 1. Kaspersky Thin Client
2. Транспортный шлюз безопасности
 1. Kaspersky Automotive Secure Gateway

??????? ??????????????, ? ??????? ????????????? ?????? ???????? ???????? ?
????????????????

????????? ? ???????????

1. Аналитика об угрозах - Kaspersky ICS Threat Intelligence
2. Кибергигиена - Kaspersky Security Awareness

3. Тренинги - Kaspersky ICS CERT Training

?????? ? ???????????

1. Анализ защищенности - Kaspersky ICS Security Assessment
2. Управляемая защита - Kaspersky Managed Detection and Response
3. Реагирование на инциденты - Kaspersky Incident Response

Kaspersky ICS EDR

Данная статья является информационной и описывает решение Kaspersky ICS EDR

??? EDR?

Технология EDR или Endpoint Detection and Response - это технология кибербезопасности, которая предназначена для мониторинга активности на устройствах (рабочие станции, сервера и тд), выявления подозрительных действий и быстрого реагирования на потенциальные инциденты.

??? Kaspersky ICS EDR?

Kaspersky ICS EDR (Industrial CyberSecurity Endpoint Detection and Response) - это решение, предназначенное для защиты промышленных объектов и АСУ ТП. В отличии от обычного EDR, который используется в IT сегменте, ICS EDR используется только в OT сегменте и позволяет защищать важные компоненты промышленных предприятий от кибеугроз. Kaspersky ICS EDR является дополнением к решение Kaspersky Industrial CyberSecurity.

???????????????????? Kaspersky ICS EDR

Функции	KICS for Nodes 4.5		KICS for Linux Nodes 2.0	
	EDR	без EDR	EDR	без EDR
YARA-проверка	+	-	N/A	N/A
KSC: Сетевая изоляция узла	+	-	N/A	N/A
KSC: Запретить запуск	+	-	N/A	N/A
KSC: Обнаружение аномалий с помощью Sigma-правил	+	-	N/A	N/A
KSC: Поиск IOC	+	-	+	-
KSC: Завершить процесс	+	-	+	-
KSC: Запустить процесс	+	-	+	-

KSC: Поместить файл на карантин	+	-	+	-
KSC: Удалить файл	+	-	+	-
KSC: Получить файл	+	-	+	-
KSC: Аудит безопасности	+	+	N/A	N/A
Интеграция с KICS for Networks: передача сведений об узле	+	+	+	+
Интеграция с KICS for Networks: аудит безопасности, анализ уязвимостей, контроль конфигурации	+	+	+	+
Интеграция с KICS for Networks: передача событий	+	+	+	+
Интеграция с KICS for Networks: передача сетевых сессий	+	+	+	+
Интеграция с KICS for Networks: передача графа атаки на узле	+	-	+	-
Реагирование из KICS for Networks: изоляция узла	+	-	+	-
Реагирование из KICS for Networks: запрет запуска	+	-	+	-
Реагирование из KICS for Networks: поместить на карантин	+	-	+	-
Реагирование из KICS for Networks: удалить файл	N/A	N/A	+	-

Функции	KICS for Nodes 4.0	KICS for Linux Nodes 1.5
---------	--------------------	--------------------------

EDR	без EDR	EDR	без EDR	
YARA-проверка	+	-	N/A	N/A
KSC: Сетевая изоляция узла	+	-	N/A	N/A
KSC: Запретить запуск	+	-	N/A	N/A
KSC: Обнаружение аномалий с помощью Sigma-правил	+	-	N/A	N/A
KSC: Поиск IOC	+	-	N/A	N/A
KSC: Завершить процесс	+	-	+	-
KSC: Запустить процесс	+	-	+	-
KSC: Поместить файл на карантин	+	+	-	-
KSC: Удалить файл	+	-	+	-
KSC: Получить файл	N/A	N/A	+	-
KSC: Аудит безопасности	+	+	N/A	N/A
Интеграция с KICS for Networks: передача сведений об узле	+	+	+	+
Интеграция с KICS for Networks: аудит безопасности, анализ уязвимостей, контроль конфигурации	+	+	+	+
Интеграция с KICS for Networks: передача событий	+	+	+	+
Интеграция с KICS for Networks: передача сетевых сессий	+	-	+	+
Интеграция с KICS for Networks: передача графа атаки на узле	+	-	N/A	N/A
Реагирование из KICS for Networks: изоляция узла	+	-	N/A	N/A

Реагирование из KICS for Networks: запрет запуска	+	-	N/A	N/A
Реагирование из KICS for Networks: поместить на карантин	+	-	N/A	N/A
Реагирование из KICS for Networks: удалить файл	N/A	N/A	N/A	N/A

????????????? ?????????????????? ????????????? KICS

????????????? ?????????????????? KICS for Nodes

Существует 2 типа лицензий для KICS for Nodes: **Workstation** (для рабочих станций) и **Server** (для серверов) как ОС Windows, так и для ОС Linux.

- Лицензии **Workstation** используется на рабочих станциях под управлением ОС семейства Windows Workstation, а также ОС Linux, выполняющих роль рабочих станций.
- Лицензии **Server**, то она используется на серверах под управлением ОС семейства Windows Server, а также ОС Linux, выполняющих роль серверов.

Минимальное количество лицензий начинается от 1 Node, срок лицензий: 1, 2, 3.

Следующий тип лицензий также, также подразделяется на 2 типа: **Workstation** (для рабочих станций) и **Server** (для серверов), но к нему еще добавляется EDR-функциональность.

Поставка лицензий предоставляет пользователю:

- Право использования ПО;
- Загрузки обновлений антивирусных баз;
- Обновления ПО KICS как в рамках текущей, так и на новые версии на момент покупки версии;
- Техническая поддержка уровня KICS Enterprise.

Приложение можно активировать двумя способами:

- С помощью файла ключа, дающего право на использование приложения в рамках коммерческой лицензии.
- С помощью кода активации для приобретения коммерческой лицензии.

По истечении срока действия коммерческой лицензии из всех компонентов и задач приложения без обновлений баз будут доступны:

- Постоянная защита файлов;
- Контроль целостности системы;
- задачи проверки по требованию.

Также есть дополнительная лицензия - это портативный сканер.

Портативный сканер позволяет выполнять проверку изолированных устройств и устаревших машин, где нет возможности установить KICS for Nodes. Портативный сканер позволяет выполнять сканирование с требуемой нагрузкой и проверять устройства на присутствие вирусов и других программ, представляющих угрозу. С помощью портативного сканера вы можете выполнять проверку нескольких устройств подряд – компонент формирует отдельный отчет для каждого проверяемого устройства.

Создается портативный сканер в интерфейсе KICS for Nodes и при создании можно указать, какие действия будут производиться над вредоносными объектами. Также с помощью портативного сканера можно производить захват трафика для анализа и выполнять аудит безопасности. Устройства, поддерживаемые портативным сканером представлены в разделе

[Программные и аппаратные требования.](#)

Лицензируется Портативный сканер как и стационарная версия - по количеству узлов, которые планируется сканировать. Для создания портативного сканера любой USB носитель с 2 ГБ места, либо защищенный токен.

???????????????????? KICS for Networks

KICS for Networks лицензируется по количеству серверов и сенсоров, на каждый из которых устанавливается ПО. 1 сервер KICS for Networks и поддерживает до 4-х интерфейсов сбора трафика (точек мониторинга). KICS for Networks Sensor – это программный продукт, устанавливаемый на согласованную аппаратную платформу (Сервер) и предоставляющий возможность сбора и предобработки трафика для дальнейшей передачи его на сервер для анализа. 1 сенсор поддерживает до 8 точек мониторинга. KICS for Networks Sensor не лицензируется и не функционирует отдельно от KICS for Networks Server.

Для KICS for Networks предусмотрены следующие типы лицензий:

- Upd&Sup – для бессрочного использования базовой функциональности программы, а также для использования функциональности обновления баз и программных модулей в течение срока действия лицензии. Данная лицензия применяется для лицензирования Сервера и для лицензирования всех используемых сенсоров программы. Минимально количество лицензий от одного, а срок лицензии доступен следующий: 1, 2, 3. Данная лицензия позволит:
 - получать обновления сигнатур IDS и иных детектирующих технологий;
 - получать обновления продукта в рамках текущей версии (Патчи и критические обновления).
 - Обновления версии ПО до последней версии.
 - Техническая поддержка уровня KICS Enterprise
- Security Audit – для бессрочного использования базовой функциональности программы, а также для использования функциональности аудита безопасности и функциональности активного опроса устройств в течение срока действия лицензии. Минимально количество лицензий от одного, а срок лицензии доступен следующий: 1, 2, 3. Лицензия активирует функционал активного опроса,

контроля конфигураций, аудита безопасности и анализа уязвимостей узлов в KICS for Networks.

- Remote Collector – для совместного использования с решением Kaspersky SD-WAN в сценариях, предусмотренных для режима интеграции. Этот тип лицензии не требует добавления лицензионного ключа в программу. Однако если вы не приобрели лицензию типа Remote Collector, вы не можете использовать KICS for Networks в режиме интеграции с решением Kaspersky SD-WAN. Дает возможность расширить до 100 точек мониторинга.

????????

??????? ?? ?????? ???? ???????? ????????????????????? ???????, ? ???? ?????? ??????
?? ?????????????? ?????????? ?????????????? Kaspersky Industrial CyberSecurity for Nodes ?
?????????, ?????? ?? ??????????? ?? ???? ???? ?????????????? ?????? ??????,

- ```

???????? ???? ??????:
- ?????? ?????????? ?????????? ??????????
- ?????????? ?????????? ??
- ?????????? ??? ? ?????? ? ?????????????? ??????
- ?????? ?????????? ?????????? ??????????????
- ?????????????????? ?????????????? ? ?????????????????? ??????????
- ?????????????? ??????
- ?????????????? ?????????????? ?????? ? ?????????????? ??????????????

```

1. ????????? ?????????????? ?????????? KICS for Nodes ? ??????????????  
 ????????????? Kaspersky Endpoint Security.

|                                                     |                |     |                  |
|-----------------------------------------------------|----------------|-----|------------------|
| <p>????????????????<br/>         ??????????????</p> | KICS for Nodes | KES | ???????????????? |
|-----------------------------------------------------|----------------|-----|------------------|

|                                                        |   |     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------|---|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>?????? ??????????</p> <p>?????????????? ???????</p> | + | -   | <p>KICS for Nodes</p> <p>?????????? ???????</p> <p>????????? ???????</p> <p>????????? ? ???</p> <p>?????????????? ???????</p> <p>??? ?????? ?????????????</p> <p>????????, ??? ?????</p> <p>?????????</p> <p>?????????????????? ?????</p> <p>????? ?????????</p> <p>?????????? ?? ?????? ?</p> <p>????????? ???????????</p> <p>?????????.</p> <p>? KES ????????? ?????</p> <p>????? ?????? ???????</p> <p>????????????????? ?????????</p> <p>??? ?????? ?????????????</p> <p>?????????.</p>        |
| <p>?????? ?? ???????????</p>                           | + | +/- | <p>?????? ???????</p> <p>?????????? ??</p> <p>????????????? ? ?????</p> <p>????????????? ???</p> <p>?????????????.</p> <p>? KES ?????? ???????</p> <p>?????? ?????? «</p> <p>?????????????? ?????????»</p> <p>/ «????????????????».</p> <p>? KICS for Nodes ?????</p> <p>????? ???????</p> <p>????????????? ???????</p> <p>?????? ?? ???????</p> <p>?????????.</p>                                                                                                                                 |
| <p>????????????? ??????? ?</p> <p>????????</p>         | + | -   | <p>?????????????? ?????????,</p> <p>????????????? ?</p> <p>????????????? ??????? ?</p> <p>????????????? ???????, ?</p> <p>????????? ?????????????,</p> <p>????????? ? ???????????</p> <p>??????.</p> <p>? KES ???????????</p> <p>?????????????.</p>                                                                                                                                                                                                                                                |
| <p>????? ???????????????</p>                           | + | -   | <p>KICS for Nodes ???</p> <p>????????????? ? KEA ?</p> <p>KICS for Networks</p> <p>????????????????? ???????</p> <p>OVAL, ?????????????</p> <p>????????????? ?????</p> <p>????????????????? ?</p> <p>compliance-????????? (?</p> <p>????????????????? ???????</p> <p>??????, ?????????????</p> <p>????????????????? ???????</p> <p>?? ?????????????????</p> <p>????????????????? ?????</p> <p>?????? ?? ??????</p> <p>????????? ??, ?</p> <p>????????????? ???????</p> <p>????? ??????? (239).</p> |

|                                           |   |     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------|---|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ??????? ???????<br>?????? ?????? ???????? | + | +/- | KICS for Nodes ?<br>??????? ?? KES<br>????????? ??? ??????<br>KSC ? ??? ?????-????<br>????????????????<br>????????? ??<br>????????????????? ???<br>???????? ?????? ?????<br>????????????? ?????? ??<br>????? ? ?????? ??????<br>???????? ?????????? (??<br>????? ??? ?<br>????????????????? ??????)<br>???????? backup<br>?????????????????<br>??????? ??? ??????????<br>??? ?? KSC. ???<br>????????????? ?????? ??<br>????? ??????? ? KES<br>?????????????<br>?????????????<br>??????????? ? KSC,<br>??????? ??????<br>????????????????? (?????<br>????????????? - ??????????<br>?????, ?????? ?????????<br>????????? ??), ??? ?????<br>??????? ??????????????<br>??????? ????????????? ? KS<br>? ??? ?????????????<br>?????????????????, ?????<br>????????????? ??????<br>??????? ?????????????<br>??????? ?????????????<br>????????????? ?????????? ?<br>????????????? ?? ? ?????<br>??????? ?????????<br>????????????? ?????????? ?<br>????, ??? ?????? ? KES<br>????????????????? ??????<br>??????? ???????. |
| ????????? ??????????                      | + | +/- | KES ??????????????<br>????????????? ?????????<br>????????????????<br>????????????, ?????? ?<br>KES ??????????????<br>?????????????<br>????????????????? ??????<br>????????????? ?????????<br>?? ?????? ??????????????<br>??? ??????????????????<br>????? ??????????????<br>????? ???????????.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|                                                                                                                  |   |     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------|---|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>???????? ????????? ?<br/> ???????????????? ??????</p>                                                         | + | -   | <p>? KES ??? ??????????<br/> ?????????????<br/> ????????? ?????????? ?<br/> ?????? ?????????????, ?<br/> ???????????????? ????<br/> ????????????? ??????????<br/> ???????. ? ?????????? ???<br/> ?? ??? (??? ? ??????<br/> ?????? ?????????????<br/> ????????????? ?? ??????<br/> ???) ????? ??????<br/> ???????????? ??????? ??<br/> ?????????????????<br/> ???????</p>                                                                                                                                                                                                                                                                                                                                          |
| <p>???????? ??????</p>                                                                                           | + | +   | <p>? KICS ?????????????<br/> ?????????????<br/> ???????????? ??????<br/> ???????? Windows, ? KES<br/> — ??? ??????????<br/> ?????</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <p>???????????? ?????????<br/> ?????????(????????<br/> ????????????<br/> ???????????? ??????? ??<br/> ?????)</p> | + | +/- | <p>????????? ?????????????<br/> ????????????????? ?????? ??<br/> ?????? ??????????<br/> ????????????? ??????????<br/> ?? ?????? ?????????????<br/> ??????, ?? ? ??<br/> ?????????????, ??????<br/> ????????? ?????????????<br/> ????????? ???<br/> ?????????????<br/> ????????????????????? ???<br/> ??. ?????????, SCADA<br/> ????????, PLC????????,<br/> ???????? ?????????????<br/> ? ?????? ?????? ??? ??<br/> ???????? ?????????<br/> ?????????. ??????<br/> ????????? ?????????? ?<br/> ????????? ?????? ???<br/> ????????????????? ?????? ?<br/> ? ?????????????<br/> ????????????? ? ??????<br/> ????????? ??.<br/> ? KES ??? ?????????<br/> ????????? ?????? ???<br/> ????????? ??????<br/> Windows.</p> |

|                                                                                         |   |     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------|---|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ????????? ??????<br>????????(????????<br>?????????<br>????????????? ?????? ??<br>?????) | + | +/- | ????????? ??????????<br>????????????????? ?????? ??<br>????? ??????????<br>????????????? ??????????<br>?? ?????? ??????????????<br>??????, ?? ? ??<br>?????????????, ??????<br>????????? ??????????<br>????????? ???<br>?????????????<br>????????????????????? ???<br>??. ?????????, SCADA-<br>?????????, PLC-?????????<br>?, ??????<br>????????????????? ?<br>????????? ?????? ?? ?<br>????????? ??????????<br>?????????????. ??????????<br>????????? ?????????????? ?<br>????????????? ?????? ??<br>????????????????? ?????? ?<br>? ??????????????<br>????????????? ? ??????<br>????????? ??.<br>? KES ??? ??????????<br>????????? ?????? ??<br>????????????? ??????<br>Windows.           |
| ?????????????<br>????????????? ?????? ??<br>?????? ????????                             | + | -   | ????????????? ??????????<br>?????????????????????<br>????????????????? ?????? ?<br>????????? ??????????????<br>????????????????? ??????????<br>????? ?????? (MD5 ???<br>SHA256) ? ??????????<br>?????????????. ??????<br>?????????????<br>????????????????? ?????? ??<br>?????? ??????????<br>????????????????? ??????????<br>????????????? ?????? ?<br>????????? ??????????????:<br>????????? ??????????????<br>????????????? ????, ??????<br>????????????????? ? ?????????;<br>? ?????????? ??????????????<br>????????????????? ????,<br>????????? ?????????????????? ?<br>?????????; ??? ?????? ?<br>????????? ??????????????<br>????????????????? ?? ?????<br>?????? ?????? ? ?????????. |

|                            |   |     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------|---|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ?????? ????????<br>Windows | + | +/- | ??????????<br>????????????? ??????????<br>????????? ??????<br>????????? ?? ??????<br>????????? ??????<br>????????????????? ??????????<br>?????? ?????????? ?<br>????????? ??????<br>?????????????????????<br>????????????? ????? ??????<br>????????????????? ?????????,<br>????????? ?? ?? ?????<br>?????????????????<br>?????????????, ?????<br>?????????????<br>?????????????????<br>?????????????????<br>?????????????????????????<br>????????? ??????<br>????????????????? ??????????<br>????????????? ?????????????<br>??? ?? ??????????<br>????????? ?? ??????????<br>? ?????? ?? ??????<br>????????? ? ?????????? ?<br>????????????????? (<br>?????????????????) ??????<br>????????????? ??????,<br>?????????<br>????????????????? ??????<br>????????????? ?? ??????<br>????????????? ?? ??????<br>????????????? ??????<br>?????????????????????<br>????????????, ??.<br>?????????????????<br>????????????????? ??????????<br>????????????????? ??????????<br>????????? ??????????<br>????????????? ????????????? ??<br>????????????? ?? ???<br>????????????? ?????? Windows<br>? ??????????????????<br>????????? ?????? ?<br>????????????? ??????????????<br>? KES ??? ??????????<br>????????? ?????? ???<br>????????????? ??????<br>Windows. |
|----------------------------|---|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                              |   |   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------|---|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>????????? ????????????</p> <p>????????? ???</p>                           | + | - | <p>????????????????? ??????</p> <p>SIMATIC S7-300</p> <p>(Siemens); SIMATIC S7-400 (Siemens); SIMATIC S7-400H ? ??????</p> <p>?????? ?</p> <p>????????????????? (</p> <p>Siemens); Schneider Electric Modicon M340; Schneider Electric Modicon M580;</p> <p>????????????? ?? ?????</p> <p>CODESYS V3; ????? ???</p> <p>210; Fastwel CPM723-01; ???????-???????? Regul</p> <p>R500; Siemens SIMATIC S7-1500; Siemens SIMATIC S7-1200; Siemens ??????</p> <p>SIPROTEC 4.</p> <p>? KES ???????????</p> <p>??????????????.</p>                                  |
| <p>????????????</p> <p>????????????????????????</p> <p>????????? ?? SNMP</p> | + | - | <p>??? ??? ?? ?????? ?</p> <p>????????? ????????</p> <p>????????????? ? ??????????</p> <p>?????????????? ?? ?????</p> <p>SNMP, ??????????,</p> <p>????????? ??????????.</p> <p>KICS for Nodes</p> <p>?????????????????</p> <p>??????????????</p> <p>????????????????????????? ?</p> <p>???????????????????? ????????</p> <p>????????????????? ?? SNMP</p> <p>??????????,</p> <p>????????????????? ??? ??????</p> <p>???????????????????? ???????</p> <p>????????????? ??????????????</p> <p>??</p> <p>?????????????????????????</p> <p>????? ?????????.</p> |

|                                                                            |   |   |                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------|---|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>????????? KICS for Nodes ? KICS for Networks</p>                        | + | - | <p>????????? ???? ????<br/> ?????????<br/> ????????? ??<br/> ????? (?????????<br/> ???, ????? ?????,<br/> ????????? ??? ?<br/> ???????) ? ??????<br/> ????????? ? ??????<br/> ????? ?? ??????<br/> ????????? ? ??????<br/> ?????????, ??????<br/> ????????? ??<br/> ?????????<br/> ????????? ?<br/> ?????????<br/> ???????????? ?? ???<br/> ????????? ?????? ??<br/> KICS for Nodes.<br/> KES ? KICS for Networks<br/> ?? ???????????.</p> |
| <p>????????? ?????? ?? Syslog ? SIEM ??????<br/> ??? ????????????? KSC</p> | + | - | <p>? KICS for Nodes<br/> ?????????<br/> ????????? ??????<br/> ?????????????????<br/> ??????? ?????????? ?<br/> SIEM ?? ??????????<br/> ????????????? ??<br/> ????? KSC.</p>                                                                                                                                                                                                                                                                |
| <p>????????? ??????<br/> ????????????? ??????<br/> ?? ? HMI-?????????</p>  | + | - | <p>? ?????? ? KICS for Nodes ??????<br/> ??????? Kaspersky Security Gateway,<br/> ?????????<br/> ????????????? ??????<br/> ?????????????<br/> ????????? ?? KSC ?<br/> ????????? ????????? ?<br/> ????????? OPC DA ?<br/> IEC 60870-5-104.</p>                                                                                                                                                                                              |
| <p>????????? ??????????<br/> ????????? ?????????? ?? USB</p>               | + | - | <p>KICS for Nodes ?????<br/> ????????????? ??????,<br/> ?????????????<br/> ????????????? ??????,<br/> ?? ?????????????? ?? ?<br/> ????????? ????????? ( ?<br/> ????????? ? USB<br/> ?????????).<br/> KES ??????????<br/> ?????? ? ??????</p>                                                                                                                                                                                               |

Нефункциональное сравнение

|          |                |     |              |
|----------|----------------|-----|--------------|
| ???????? | KICS for Nodes | KES | ???????????? |
|----------|----------------|-----|--------------|

|                                   |   |   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|---|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ????????? ??????????<br>????????? | + | - | ? ?????? KICS for Nodes<br>?????????<br>?????????????????<br>??????????????, ??????<br>????????? ??????????<br>?????????????<br>????????????? ??????????<br>?? ??????????<br>????????????? ??????<br>?? ?? ??????<br>????????, ?? ? ??<br>????????? ?????????? ?<br>?????????????, ?????????<br>???????? ??????????<br>?????. ??????????????<br>????? ??????????????<br>?????????????<br>????????????? ??????????,<br>?? ?????? ??????????<br>????? ??????????????<br>?????????<br>????????????????? ??????<br>????????????????? ?????????,<br>????????? ?????? ??<br>????????????? ?????????? ?<br>????????????? ??????,<br>????????????? ? ??? ??.<br>?????, ? KICS for Nodes<br>????????? ?????????????<br>????????????????? ??????<br>????????????????? ??,<br>????????????????? ?? ?????<br>????????? ?? ??????????<br>??, ??? ????????? ??????<br>?????????<br>?????????????????<br>?????????<br>KES ?? ??????????????<br>????????????????? ??????????<br>?????????????. |
|-----------------------------------|---|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                          |   |     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------|---|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>????????? ??????? ??</p> <p>?????????????</p> <p>??????????</p>                       | + | -   | <p>KICS for Nodes ?????</p> <p>???? ?????????? ??</p> <p>????? ?? ? ? ??????????</p> <p>???????? ???</p> <p>???????????????????</p> <p>?????????????, ???</p> <p>????????????? ??????????</p> <p>????? ??????????????</p> <p>????????? ??????</p> <p>?????????, ??? ?????</p> <p>????????? ????? ?????</p> <p>???? ???? ? ? ???? ?</p> <p>??, ?? ???? ??????????</p> <p>?? ???????. ??</p> <p>?????????</p> <p>????????????????? ?????</p> <p>?????????????????</p> <p>????????? ???</p> <p>???????????? ???? ?????</p> <p>????? ??? ??</p> |
| <p>????????? ?? ??????????</p> <p>? ?????????????? ??????</p>                            | + | -/+ | <p>? KES ?? ?????????? ?</p> <p>????????????? ??????</p> <p>????????? ??????????,</p> <p>????????????? ? ?? ??:</p> <p>?????? ?? ??????????</p> <p>?????, ?????? ?? ???-</p> <p>?????, ?????? ??</p> <p>????????? ?????, ??????</p> <p>????????????, ?????? ??</p> <p>?????????????. ??????????</p> <p>???????????? ??</p> <p>???????????? ?????</p> <p>?????????, ????</p> <p>????????? ? ??????</p> <p>?????????????????.</p> <p>? KICS for Nodes ?</p> <p>????????????? ??????</p> <p>????????? ??????????</p> <p>AMSI-?????.</p>        |
| <p>????????????? ?????????</p> <p>????????????????? ?? (</p> <p>????????? ?????? ??)</p> | + | -   | <p>KICS for Nodes</p> <p>?????????????</p> <p>????????????? ?????????</p> <p>????????????? ??????</p> <p>????????????? Windows XP</p> <p>SP2, Windows</p> <p>Embedded, Windows</p> <p>Server 2003 SP1. ???</p> <p>????????? ????????? ???</p> <p>??, ??????? ????? 10</p> <p>?? ? ?????? ?? ?? ??</p> <p>????????</p> <p>????????????????? ?</p> <p>???????????????? ????.</p> <p>??? ?????????? ?????????</p> <p>???????????????? ??? ??</p> <p>??? ????????????? ??????</p> <p>?????????????????</p> <p>????????????????.</p>             |

|                                                                                                                         |   |   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>????????? ? ????????</p> <p>????????? ??</p> <p>?????????????? ??</p>                                                | + | - | <p>????????????</p> <p>????????????????</p> <p>???????????????? ??</p> <p>????????? ??????????</p> <p>????? ??????????????</p> <p>????????? ??? ?</p> <p>????????? ??????????????</p> <p>?? ??</p>                                                                                                                                                                                                                                                                                                |
| <p>????????? ??????????????</p> <p>??? ?? ????????????</p> <p>??????? ?????????????? ??</p> <p>????????????????? ??</p> | + | - | <p>?????????????</p> <p>????????????? ??????</p> <p>??????? ?????????? ?</p> <p>???????????</p> <p>???????????????????? ?? ?</p> <p>??????? ??? ?????????????</p> <p>?????????</p> <p>???????????????????? ??</p> <p>????????????? ?????</p> <p>????????? ? ??????????????</p> <p>?????????????</p> <p>????????????????? ??? ???</p> <p>KICS for Nodes ??????????</p> <p>?????????????????</p> <p>????????? ?? ?????????????</p> <p>??????? ?????????????? ??</p> <p>???????????????????? ??.</p> |
| <p>???????????????</p> <p>????????????????? ?</p> <p>????????????? ??? ??</p>                                           | + | - | <p>???????????????</p> <p>????????????????? ??????????</p> <p>????????????? ? ??????????????</p> <p>???????????????????? ??</p> <p>???????????????????? ??</p> <p>??????????????????,</p> <p>????????????????? ??????????</p> <p>?????????????????</p> <p>??????????????????,</p> <p>????????????? ??????????:</p> <p><a href="https://ics.kaspersky.ru/resources/#certification">https://ics.kaspersky.ru/resources/#certification</a>.</p>                                                      |
| <p>????????????????????</p> <p>?????????????? ??</p> <p>????????????? ? ??????????????</p> <p>????????????? ????</p>    | + | - | <p>??? ?????????,</p> <p>?????????????????</p> <p>????????????????? ?? ??????</p> <p>????????????? ??????????????</p> <p>?? ?????????? ??????????????</p> <p>??????? ??????????????????</p> <p>??, ? ??????</p> <p>????????????????? ??</p> <p>????????????? ??????????????</p> <p>????? (????????????? ???</p> <p>??????, ?????).</p> <p>?????????????</p> <p>????????????????? ??????????????</p> <p>????????????? ??? ?</p> <p>??????? ??????????????????</p> <p>?????????</p>                 |

|                                            |   |   |                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------|---|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>????????? ?? ?????</p> <p>?????????</p> | + | - | <p>????????????</p> <p>????????????</p> <p>????????????? ?????</p> <p>????????? ?? ?????</p> <p>????????? ??????</p> <p>????? ??????????</p> <p>????????????? ?????</p> <p>????????????????? ??????</p> <p>?? ????? ?? ????????,</p> <p>????????? ??????</p> <p>????????????? ??</p> <p>?????????.</p> |
|--------------------------------------------|---|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Сертификация

| ????                                     | KICS for Nodes           | KES                      | ?????????????                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|--------------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>????????????? ?????</p> <p>??????</p> | <p>±</p> <p>(??????)</p> | <p>±</p> <p>(??????)</p> | <p>KICS for Nodes ?????</p> <p>????????????? ?????</p> <p>??????, ??????????????</p> <p>????????????? ??????</p> <p>????????????? ?</p> <p>?????????</p> <p>????????????? ??????,</p> <p>???????? ?????? ??? (??</p> <p>2-?? ??????),</p> <p>????????????? ?????? (</p> <p>?? 2-?? ??????), ??????</p> <p>?????? ??? (?? 2-??</p> <p>??????).</p> |
| <p>????????????? ??</p> <p>??????</p>    |                          |                          | <p>KICS for Nodes ?????</p> <p>????????????? ?? ??????,</p> <p>?????????????????</p> <p>????????????????? ??????</p> <p>????????????????? ?</p> <p>?????????????</p> <p>?????????????</p> <p>????????????? ??2.</p>                                                                                                                               |

2. ????????????????? KICS for Nodes ? ????????????????? ??????????.

Совместимость средств кибербезопасности с оборудованием и ПО промышленных вендоров — ключевой аспект при создании защищенной инфраструктуры предприятия. В отличие от традиционных ИТ-систем, где обновления и изменения конфигурации — обычное дело, промышленный сегмент крайне чувствителен к любым вмешательствам. На предприятиях применяются решения различных производителей — от систем автоматизации и SCADA до специализированных контроллеров. Каждое из них уникально, имеет свои требования к ресурсам и ограничения на установку стороннего ПО. Неправильная работа защитных программ может нарушить технологические процессы, привести к простоям оборудования и финансовым потерям. Поэтому промышленный антивирус должен не только надежно защищать, но и подтверждать совместимость с решениями ведущих вендоров. Этого можно достичь через тестирования, сертификации и тесное

сотрудничество разработчиков защитных средств с производителями промышленного оборудования.

Для ознакомления с перечнем сертификатов соответствия KICS for Nodes и сторонних вендоров перейдите по [ссылке](#).

### 3. ????????????? ?????? ? ????????????? ?????????????.

С ростом киберугроз и усилением требований к защите критически важной информационной инфраструктуры соответствие средств информационной безопасности нормативам становится обязательным условием для их использования на промышленных предприятиях. Регуляторы и отраслевые организации разрабатывают стандарты и рекомендации для обеспечения устойчивости, надежности и защищенности технологических процессов. Промышленные системы, особенно автоматизированные системы управления технологическими процессами (АСУ ТП), выдвигают особые требования к средствам защиты. Эти решения должны не только эффективно противостоять современным угрозам, но и соответствовать нормам, регулирующим их применение в критически важных средах. Это особенно важно для предприятий энергетики, нефтегазовой отрасли, транспорта и других сегментов, входящих в объекты критической инфраструктуры. Промышленный антивирус, соответствующий требованиям регуляторов, проходит сертификацию, которая подтверждает его безопасность, надежность и корректность работы в специализированной среде. Кроме того, соответствие международным и национальным стандартам облегчает процессы аудита, внедрения и эксплуатации решений, а также снижает риски для бизнеса.

Для ознакомления с перечнем сертификатов соответствия регуляторным требованиям и нормам можно ознакомиться перейдя по [ссылке](#).

Для более детального изучения требований приказа ФСТЭК №239 и их выполнения с помощью KICS for Nodes рекомендуем ознакомиться со статьей "[Реализация мер 239 приказа ФСТЭК](#)".