

*А.С. Мельников (ООО «Сименс»),
С.И. Палтов (АО «Лаборатория Касперского»)*

Обеспечение безопасности SCADA-системы WinCC OA средствами WinCC OA и KICS

Приводится сопоставление указанных в Приказе ФСТЭК от 25.12.2017 N 239 мер по обеспечению безопасности значимых объектов и функции безопасности SCADA-системы SIMATIC WinCC Open Architecture и решения по безопасности Kaspersky Industrial CyberSecurity, которые могут быть использованы при реализации данных мер.

Ключевые слова: информационная безопасность, кибербезопасность, SCADA-система, мониторинг промышленных сетей, объект критической информационной инфраструктуры.

*Мельников Андрей Сергеевич – главный инженер по интеграции проекта ООО «Сименс»,
Палтов Сергей Игоревич – руководитель группы по развитию архитектуры решений АО «Лаборатория Касперского».*

Список литературы

- 1. Космин А.С., Серов А.Ю., Соловьев С.Ю. Мониторинг производственных линий с SIMATIC WinCC Open Architecture // Control Engineering Россия. 2017. №6 (72).*
- 2. Мельников А.С., Соловьев С.Ю. Обеспечение информационной безопасности при применении SCADA-Системы SIMATIC WINCC Open Architecture // Автоматизация в промышленности. 2017. №7.*
- 3. Серов А.Ю., Соловьев С.Ю. Новое в WinCC OA версии 3.16: инженерная эффективность, производительность и безопасность как ключевые характеристики SCADA-системы в эпоху цифровой трансформации // ИСУП. 2018. № 3(75).*

Melnikov A.S., Paltov S.I. Ensuring WinCC OA SCADA security by means of WinCC OA and KICS tools

The paper compares the security measures listed in the FSTEC (Federal Service for Technical and Export Control) Order #239 of 25.12.2017 against the security functions of SIMATIC WinCC Open Architecture SCADA system and discusses Kaspersky Industrial CyberSecurity solutions that may be used to implement these security measures.

Keywords: information security, cybersecurity, SCADA system, monitoring of industrial networks, object of critical information infrastructure.