

DOI: 10.25728/avtprom.2024.09.13

А.А. Винявский («Лаборатория Касперского»)

Industrial Internet of Things: риски и защита в цифровую эпоху

Сформулированы проблемы в области кибербезопасности, которые характерны для устройств Industrial Internet of Things. Рассматривается подход «Лаборатории Касперского» к созданию конструктивно безопасных систем – кибериммунитет. Описываются практические преимущества кибериммунитета для промышленных предприятий на примере шлюза промышленных данных Kaspersky IoT Secure Gateway.

Ключевые слова: Industrial Internet of Things, кибербезопасность, шлюз промышленных данных, кибериммунитет.

Винявский Александр Анатольевич – технологический евангелист «Лаборатории Касперского».

Список литературы

1. Contos B. *The secret, insecure life of Security Cameras*. Forbes. 2023. <https://www.forbes.com>
2. O'Donnell L. *More Than Half of IoT Devices Vulnerable to Severe Attacks*. Threat Post. 2020. <https://threatpost.com>
3. Biggs S., Lee D., Heiser G. *The Jury Is In: Monolithic OS Design Is Flawed: Microkernel-based Designs Improve Security*. August. 2018.

Vinyavsky A.A. Industrial Internet of Things: risks and protection in the digital age

Cyber security challenges typical for IIoT devices are formulated. The concept of cyber immunity offered by Kaspersky Lab as an approach to the design of structurally secure systems is discussed. Practical advantages of cyber immunity for industrial sites are described by example of Kaspersky IoT Secure Gateway.

Keywords: *Industrial Internet of Things, cyber security, industrial data gateway, cyber immunity.*