UDC 65.06

CHECKPOINTS AND INDUSTRIAL ESPIONAGE IN THE PHARMACEUTICAL SECTOR IN THE CONTEXT OF DIGITAL TRANSFORMATION

Hazima M.W. (ITMO)
Scientific supervisor – Candidate of Economic Sciences, senior lecturer Kahn E.N.
(ITMO)

Introduction. In the dynamic landscape of the pharmaceutical industry, the nexus between checkpoints personnel and industrial espionage poses a formidable challenge. As pharmaceutical companies undergo rapid digital transformation, the burden on checkpoint personnel has become increasingly complex. This research delves into the existing disparities between the capabilities of checkpoint personnel and industrial espionage actors, proposing a tailored solution in the form of a unified security ecosystem. This framework aims to streamline tasks, enhance efficiency, and fortify the sector against emerging digital threats. The current situation is that checkpoints personnel, tasked with a myriad of responsibilities including access control, physical surveillance, and package inspection, often find themselves overwhelmed by the complexity of their duties. Compounded by the use of outdated, non-integrated systems and platforms, these staff struggle to manage the diverse range of tasks required to maintain a comprehensive security posture. Unlike industrial espionage actors who can focus solely on the singular task of compromising sensitive data and information theft. Physical theft and loss is considered one of the top three types of breaches in the healthcare sector, as physical theft and loss, abuse of privileges, and miscellaneous errors represent 80% of the total breaches in the healthcare sector [1].

A solution is imperative to empower these personnel, allowing them to refocus on physical threats while efficiently managing the digital landscape.

Main body. The cornerstone of the proposed solution is a unified security ecosystem, designed to optimize the efficiency of checkpoints in the pharmaceutical sector. Key components include:

- Centralized access control: Implement a centralized access control system that integrates physical and digital access points. This ensures a seamless flow of authorized personnel while minimizing the risk of unauthorized entry.
- AI-driven threat detection: Integrate AI-driven threat detection algorithms to analyse patterns and identify potential security risks. According to the Consumer Technology Association, 44% of organizations across the globe are implementing AI applications to detect and deter security intrusions [2]. AI collaborates with surveillance cameras, automatically flagging anomalies and allowing personnel to focus more on physical security concerns.
- Task automation: Automate routine tasks, such as identity verification and basic screenings, to alleviate the workload on checkpoints. This automation allows personnel to concentrate on high-priority tasks and enhances overall operational efficiency.
- Real-time communication hub: Establish a real-time communication hub that connects checkpoints personnel, AI systems, and cybersecurity experts. This collaborative platform facilitates swift information exchange, enabling a coordinated response to emerging threats.

The Implementation Proposals are the followings:

1- Develop a prototype of the unified security ecosystem and conduct pilot programs within pharmaceutical companies to assess its effectiveness in real-world scenarios.

2- Foster collaboration between checkpoint personnel, AI experts, and cybersecurity professionals to fine-tune and optimize the unified security ecosystem.

3- Implement training programs to familiarize checkpoint personnel with the unified security ecosystem, ensuring seamless integration into existing workflows.

Conclusions. The proposed unified security ecosystem offers a transformative solution to the existing challenges faced by checkpoint personnel in securing pharmaceutical assets. By centralizing access control, integrating AI-driven threat detection, and automating routine tasks, this ecosystem

empowers personnel to effectively manage both physical and digital security concerns. This proposal lays the foundation for a resilient, adaptive, and streamlined security infrastructure in the pharmaceutical sector.

List of used sources:

1. 2017 Data Breach Investigations Report // Verizon. – 2017. – 10th Edition. – P. 76. Available at: https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf
2. Artificial Intelligence in Security Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029) // Mordor Intelligence. – 2024. Available at: https://www.mordorintelligence.com/industry-reports/artificial-intelligence-in-security-market