ZAMONAVIY HUQUQSHUNOSLIKNING AKTUAL MUAMMOLARI

XXI-RESPUBLIKA ILMIY-AMALIY KONFERENSIYA

YAKUNLARI BO'YICHA ILMIY ISHLAR TO'PLAMI

Issue – 12(2025) Available at www.uznauka.uz

MODERN THEORETICAL APPROACHES OF CYBERSECURITY OF PROTECTED FACILITIES INFRASTRUCTURE

Saidov Bakhodirkhoja Nasirkhojaevich

The leading specialist of the Cyber Security Center of the Main Department of Intimidation of the National Guard of the Republic of Uzbekistan

bahodirkhujasaidov@gmail.com

Abstract: *this article explores modern theoretical approaches to the cybersecurity of protected facilities infrastructure. It analyzes current threats and vulnerabilities inherent in critical infrastructure systems and examines advanced security frameworks and principles designed to mitigate cyber risks. Emphasis is placed on integrating technology, policy, and human factors to create resilient defense mechanisms. The study also highlights the importance of proactive risk management and international best practices for safeguarding sensitive installations.*

Keywords: *cybersecurity, protected facilities, infrastructure security, threat management, cyber risk, defense frameworks, critical infrastructure.*

Introduction

In an era of increasing digitalization, the cybersecurity of protected facilities' infrastructure has become a crucial concern. These facilities, which include government buildings, energy grids, and transportation hubs, face escalating cyber threats that can disrupt operations and compromise national security. Traditional protection methods are often insufficient against sophisticated cyberattacks, necessitating modern theoretical approaches that encompass not only technical solutions but also organizational and strategic dimensions. This article discusses key concepts and methodologies underpinning contemporary

cybersecurity strategies, aiming to enhance the protection and resilience of critical infrastructure.

Main part

The conceptual framework for cybersecurity for protected infrastructure under civil law has undergone significant changes in recent decades. Traditional approaches to security have evolved from purely physical defense mechanisms to sophisticated cyber-physical systems that combat modern technological threats. This evolution reflects fundamental changes in the concept, protection, and regulation of protected infrastructure within legal systems. International frameworks developed by organizations such as the International Institute for Protected Infrastructure Protection and the ITU Cybersecurity Division have played a significant role in shaping these changes.

The process of ensuring the security of protected facilities has undergone profound changes, especially from the 1980s to the 2010s, when a transition began to be made to cyber-physical protection integrated with purely physical security mechanisms. The first reports of cyber vulnerabilities in infrastructure systems appeared in the late 1980s[1].

By the mid-2000s, the emergence of increasingly sophisticated cyber threats targeting infrastructure and the weakness of the existing international legal framework had attracted the attention of scholars. Studies published in international journals also highlighted significant gaps between technical security requirements and legal norms. At the same time, technical standards bodies began

[1]Anderson, R. J. (1994). Why cryptosystems fail. Communications of the ACM, 37(11), 32-40. https://doi.org/10.1145/188699.188719

to develop specific guidelines for the security of industrial control systems, which were initially advisory in nature.

This historical development shows how the security of protected facilities has evolved from a primarily physical problem to one requiring integrated cyber-physical approaches that have undergone a parallel evolution within the framework of civil law. The transition has paved the way for the emergence of more comprehensive approaches as technology has continued to develop and cyber threats have become more sophisticated.

The period from 2010 to 2018 saw a significant integration of cybersecurity into existing infrastructures, reflecting the fact that physical and digital security can no longer be considered in isolation. At the same time, legislation has begun to clearly define cybersecurity requirements for protected infrastructure, as exemplified by the European Union's Network and Information Security Directive (2016/1148), which imposes a number of cybersecurity obligations on service operators.

Cyberattacks have had a significant impact on the development of cybersecurity legislation. The Stuxnet incident, which targeted Iran's nuclear facilities, demonstrated how sophisticated cyber weapons can damage protected infrastructure[2].

Effective protection of protected infrastructure requires seamless integration between technical security standards and legislative frameworks, creating a regulatory environment that both sets out clear obligations and provides practical guidance for implementation.

[2]Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40. https://doi.org/10.1080/00396338.2011.555586

Harmonizing technical standards with the legislative framework remains a particularly challenging task in Central Asian legal systems, which must balance international compliance with diverse national regulatory traditions. The comparative analysis revealed significant differences in how technical standards are incorporated into the legal frameworks in the region, with some jurisdictions adopting voluntary approaches to compliance while others establish mandatory certification requirements. These differences create significant complexity for organizations operating across multiple jurisdictions in Central Asia.

Economic risks are important dimensions of the cybersecurity of protected entities, fundamentally influencing investment decisions, the allocation of responsibilities, and the overall security posture. The World Bank's study on the economics of cybersecurity shows that market failures often undermine optimal security investments, as organizations often underinvest in defenses due to negative externalities and information asymmetries. These market dynamics pose particular challenges for secure entities, where security failures can have broader societal impacts beyond the direct losses to the attacked organization[3].

As cyberthreats have increased, insurance mechanisms have become an important tool for managing cyber risks, but significant challenges remain in developing markets for protecting cyber-physical systems.

While significant challenges remain in developing accurate models for high-impact events typical of attacks on secure facilities, methodologies for quantifying cyber risks have advanced significantly. Systematic approaches, such as the

[3]Suter, M. (2018). Economics of cybersecurity. In M. Christen, B. Gordijn, & M. Loi (Eds.), The ethics of cybersecurity (pp. 195-210). Springer.

Factorial Analysis of Information Risk (FAIR) methodology, provide a framework for estimating potential losses, influencing insurance and investment decisions.[4].

Conclusion

Modern theoretical approaches to cybersecurity of protected facilities infrastructure emphasize a holistic and adaptive strategy that combines technological innovation, comprehensive risk assessment, and coordinated policy measures. Implementing these approaches enhances the ability to detect, prevent, and respond to emerging cyber threats effectively. Continuous improvement, workforce training, and alignment with international standards are vital for maintaining robust security postures. Ultimately, these strategies contribute to ensuring the operational continuity and safety of protected infrastructures in an increasingly complex cyber threat landscape.

FOYDALANILGAN ADABIYOTLAR

1. Anderson, R. J. (1994). Why cryptosystems fail. Communications of the ACM, 37(11), 32-40. https://doi.org/10.1145/188699.188719
2. Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40. https://doi.org/10.1080/00396338.2011.555586
3. Suter, M. (2018). Economics of cybersecurity. In M. Christen, B. Gordijn, & M. Loi (Eds.), The ethics of cybersecurity (pp. 195-210). Springer.
4. FAIR Institute. (2019). Fair risk analysis methodology. Factor Analysis of Information Risk Institute.

[4]FAIR Institute. (2019). Fair risk analysis methodology. Factor Analysis of Information Risk Institute.