UDC [502.174:556.53](043.2)=111

Yurii V. Perehniak
Nataliia M. Hadaichuk

CYBERSECURITY IN THE AGE OF DIGITAL TRANSFORMATION: THREATS AND PROTECTION MEASURES

Vinnytsia National Technical University

Анотація

Дана доповідь присвячена проблемі кібербезпеки в епоху цифрової трансформації. Зростаюча залежність від інформаційних технологій створює нові загрози для організацій і суспільства в цілому. У рамках доповіді будуть розглянуті основні загрози кібербезпеці, такі як кібератаки, витоки даних та шкідливе програмне забезпечення. Також будуть обговорені заходи захисту, зокрема роль фізичних ключів шифрування у забезпеченні безпеки інформаційних систем. Презентація покликана підвищити усвідомленість про кібербезпеку та надати практичні поради зі забезпечення безпеки в епоху цифрової трансформації.

Ключові слова: кібербезпека, цифрова трансформація, загрози, захист, кібератаки, витоки даних, шкідливе програмне забезпечення, фізичні ключі шифрування.

Abstract

This presentation focuses on the issue of cybersecurity in the era of digital transformation. The increasing reliance on information technologies creates new threats for organizations and society as a whole. The presentation will explore key cybersecurity threats, such as cyberattacks, data breaches, and malicious software. Additionally, it will discuss protective measures, including the role of physical encryption keys in securing information systems. The presentation aims to raise awareness about cybersecurity and provide practical advice for ensuring security in the era of digital transformation.

Key words: cybersecurity, digital transformation, threats, protection, cyberattacks, data breaches, malicious software, physical encryption keys.

Introduction

In the digital age, cybersecurity has become a paramount concern as organizations and individuals navigate the challenges of digital transformation. The reliance on information technologies and interconnected systems has brought about new and sophisticated cyber threats. This presentation explores the topic of cybersecurity in the context of digital transformation, focusing on the role of physical encryption keys in protecting sensitive information.

The presentation discusses the evolving nature of cyber threats, including traditional attacks and advanced techniques such as malware and phishing. It highlights the potential consequences of these threats, such as financial loss and reputational damage. Additionally, the presentation examines the impact of digital transformation on cybersecurity, considering the vulnerabilities introduced by new technologies.

One key aspect of the presentation is the role of physical encryption keys in enhancing cybersecurity. Encryption keys play a crucial role in securing data and communications. The presentation explores the principles of encryption and how physical keys provide an additional layer of protection through secure storage and authorized access to cryptographic keys.

By raising awareness of cybersecurity challenges and discussing the importance of physical encryption keys, this presentation aims to equip organizations with insights and strategies to strengthen their cybersecurity posture in the digital transformation era.

Research Result

The research conducted in the field of cybersecurity in the era of digital transformation has provided valuable insights into various aspects of this domain. Here are the key findings:

Cyber Threat Landscape: Extensive research reveals that the cyber threat landscape has undergone significant changes in recent years. Cyberattacks have become more frequent and sophisticated, with attackers employing advanced techniques to breach organizational defenses. Ransomware, advanced persistent threats (APTs), and social engineering attacks are on the rise.

Impact of Cyberattacks: The impact of cyberattacks on organizations is far-reaching. Research consistently demonstrates that these incidents can lead to substantial financial losses, operational disruptions, and reputational damage. The direct financial costs associated with incident response, remediation, and legal implications can be substantial. Indirect costs include a loss of customer trust, decreased market share, and long-term damage to brand reputation.

Role of Encryption: Encryption is recognized as a crucial security measure in protecting sensitive information. Research consistently highlights the effectiveness of encryption in safeguarding data confidentiality, integrity, and authenticity. Encryption algorithms mathematically transform data into unreadable formats, rendering it useless to unauthorized individuals who gain access to it.

Importance of Physical Encryption Keys: Physical encryption keys play a pivotal role in enhancing cybersecurity. Research emphasizes their significance in providing an additional layer of protection for cryptographic keys. Physical keys, such as USB tokens or smart cards, securely store encryption keys and require physical possession for their use. They protect against unauthorized key duplication or theft, ensuring that only authorized individuals can access sensitive data.

Benefits of Key Management: Effective key management practices are crucial for maintaining strong encryption security. Research highlights the benefits of centralized key management systems, which enable organizations to maintain control over encryption keys, monitor their usage, and enforce access controls. These systems facilitate secure key distribution, rotation, and revocation, reducing the risk of unauthorized key exposure.

User Acceptance and Usability: User acceptance and usability are critical factors for the successful adoption of physical encryption keys. Research emphasizes the importance of ensuring that the use of physical keys does not impose significant burdens on users. User-friendly interfaces, seamless integration into existing workflows, and clear instructions contribute to a positive user experience and encourage widespread implementation.

Compliance and Regulatory Considerations: The research underscores the growing importance of compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) and industry-specific standards. Physical encryption keys can assist organizations in meeting regulatory requirements by providing secure key storage and management mechanisms, which are often mandated for protecting sensitive data.

In summary, the research provides valuable insights into the evolving cyber threat landscape and the impact of cyberattacks on organizations. Encryption, including the use of physical encryption keys, is recognized as a crucial security measure. Implementing proper key management practices, ensuring user acceptance and usability, and complying with regulatory frameworks are essential steps for organizations aiming to protect sensitive data and maintain the trust of their stakeholders.

Conclusion

In summary, the research highlights the importance of cybersecurity in the era of digital transformation. Key findings include the evolving cyber threat landscape, the impact of cyberattacks on organizations, the role of encryption and physical encryption keys in enhancing security, the benefits of proper key management practices, considerations for user acceptance and usability, and the significance of compliance with data protection regulations. These insights emphasize the need for organizations to prioritize cybersecurity measures to protect sensitive information, mitigate cyber threats, and maintain stakeholder trust.

REFERENCES

1. Main types of cybersecurity in the context of personal data protection and processing URL: https://bsoprivacygroup.com/cyber-cecurity/ (дата звернення: 16.06.2023).

2. Cyber security and risks of digital transformation of companies URL: https://kniga.biz.ua/pdf/31947-kiberbezpeka-1.pdf (дата звернення: 16.06.2023).

Перегняк Юрій Валерійович – студент групи КІВТ-22м, факультет інформаційних електронних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: yuraperehniak@gmail.com

Науковий керівник: Гадайчук Наталія Миколаївна – старший викладач кафедри іноземних мов, Вінницький національний технічний університет, м.Вінниця, e-mail: hadaichuk@vntu.edu.ua

Perehniak Yurii Valerievich – student of the group KIVT-22m, Faculty of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: yuraperehniak@gmail.com

Scientific supervisor: Hadaichuk Nataliia Mykolaivna – Senior Lecturer, Department of Foreign Languages, Vinnytsia National Technical University, Vinnytsia, e-mail: hadaichuk@vntu.edu.ua