

CYBERSECURITY IN SOFTWARE DEVELOPMENT: MODERN THREATS AND DEFENSE STRATEGIES

Vinnitsia National Technical University

Анотація

Стаття присвячена дослідженню актуальних проблем кібербезпеки в процесі проєктування та розробки програмного забезпечення. Розглядаються основні типи вразливостей, такі як SQL-ін'єкції та витік даних, а також методи їх запобігання на ранніх етапах життєвого циклу розробки. Особлива увага приділяється концепції DevSecOps та важливості впровадження криптографічних методів захисту інформації для створення надійних цифрових продуктів.

Ключові слова: кібербезпека, розробка ПЗ, DevSecOps, шифрування, вразливості системи.

Abstract

The article is devoted to the study of current cybersecurity issues in the process of software design and development. It examines the main types of vulnerabilities, such as SQL injections and data breaches, as well as methods to prevent them at the early stages of the development life cycle. Special focus is placed on the DevSecOps concept and the importance of implementing cryptographic data protection methods to create reliable digital products.

Key words: cybersecurity, software engineering, DevSecOps, encryption, system vulnerabilities.

Introduction

In the digital age, cybersecurity has become a critical aspect of software engineering. As software systems become more complex, they also become more vulnerable to sophisticated cyberattacks. Unlike traditional development, where security was often considered only at the final stage, modern engineering requires a "security-by-design" approach. Features such as multi-factor authentication and secure coding standards are now essential for protecting user data. Integrating security measures from the very beginning not only prevents financial losses but also builds trust between developers and users.

Research results

One of the most important aspects of modern software engineering is the identification and mitigation of common security threats.

[1] According to recent reports, injection flaws and broken access control remain the top risks for web applications.

[2] This highlights the need for developers to use automated scanning tools to detect vulnerabilities during the coding process.

Moreover, the shift towards cloud-based architectures has introduced new challenges in data protection and network security.

Another vital feature of secure development is the implementation of the DevSecOps methodology, which integrates security practices into every phase of the development cycle.

[3] By automating security checks in the CI/CD pipeline, development teams can identify potential risks before the software is even deployed.

Many developers start by using basic encryption for passwords and gradually move on to implementing complex Zero Trust architectures.

Understanding cryptography and secure communication protocols is becoming a mandatory skill for software engineers, requiring deep logical analysis and attention to detail.

In addition to technical solutions, cybersecurity also involves human factors, such as training developers to recognize social engineering tactics.

The industry also places high value on open-source security, as many modern projects rely on third-party libraries that may contain hidden bugs.

[4] Furthermore, global security standards like ISO/IEC 27001 provide a framework for organizations to manage their information security risks effectively.

Conclusion

Cybersecurity is no longer an optional feature – it is the foundation of high-quality software engineering. The ability to anticipate threats and implement robust defense mechanisms allows for the creation of resilient and trustworthy systems. Beyond technical implementation, security culture encourages responsibility, continuous learning, and strategic planning within development teams. As cyber threats continue to evolve, the role of secure coding practices and proactive defense will remain central to the future of technology.

REFERENCES

- 1.OWASP Top 10: Critical Web Application Security Risks [Електронний ресурс] – Режим доступу: <https://owasp.org/www-project-top-ten/>.
- 2.Cybersecurity & Infrastructure Security Agency (CISA) Resources [Електронний ресурс] – Режим доступу: <https://www.cisa.gov/resources-tools>.
- 3.DevSecOps: Integrating Security into DevOps [Електронний ресурс] – Режим доступу: <https://www.redhat.com/en/topics/devops/what-is-devsecops>
- 4.ISO/IEC 27001: Information Security Management [Електронний ресурс] – Режим доступу: <https://www.iso.org/iso-iec-27001-information-security.html>.

Нечипорук Софія Сергіївна – студентка групи 2ПІ-25б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: sonaneciporuk@gmail.com.

Науковий керівник: **Чопляк Вікторія Володимирівна** – викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, м. Вінниця, e-mail: nikavnuchkova@gmail.com.

Sofia S. Nechiporuk – a student of 2PI-25b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: sonaneciporuk@gmail.com.

Scientific Supervisor: **Victoria V. Chopliak** – teacher of English, Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia, e-mail: nikavnuchkova@gmail.com.