А. В. Скіп

ІДЕНТИФІКАЦІЯ ПРОЦЕСІВ КІБЕРБЕЗПЕКИ В ЛАНЦЮГАХ ПОСТАЧАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Вінницький національний технічний університет

Анотація:
Розглянуто ідентифікацію процесів кібербезпеки в ланцюгах постачання програмного забезпечення (ПЗ). Запропоновано математичну модель на основі множинних описів та графів залежностей, що дозволяє структурувати процеси безпеки, оцінити ризики та реалізувати захисні заходи. досліджено ідентифікацію процесів кібербезпеки в ланцюгах постачання програмного забезпечення (ПЗ). Представлено математичну модель, що базується на множинних описах та графах залежностей, яка дозволяє структуровано оцінити ризики та реалізувати захисні заходи. Аналізуються загрози, пов'язані з компрометацією компонентів на різних етапах життєвого циклу ПЗ, зокрема уразливості відкритого коду, атаки на ланцюг постачання, а також загрози, що виникають у процесах інтеграції та розгортання.

Ключові слова: кібербезпека, ланцюг постачання програмного забезпечення, математичний опис, процеси кібербезпеки, управління ризиками.

Abstract:
The paper addresses cybersecurity in software supply chains, presenting a mathematical model based on set descriptions and dependency graphs for structured assessment of security risks and protective measures. The identification of cybersecurity processes in software supply chains is considered. A mathematical model based on set descriptions and dependency graphs is proposed, allowing for the structuring of security processes, risk assessment, and the implementation of protective measures. The study investigates the identification of cybersecurity processes within software supply chains. A mathematical model, based on multiple descriptions and dependency graphs, is presented, enabling a structured risk assessment and the implementation of protective measures. The analysis focuses on threats associated with component compromise at various stages of the software lifecycle, including open-source vulnerabilities, supply chain attacks, and threats arising during integration and deployment processes.

Keywords: cybersecurity, software supply chain, cybersecurity processes, mathematical model, risk management.

Вступ

Останніми роками стрімко зростає кількість та масштаб атак на ланцюги постачання програмного забезпечення (ПЗ). Це обумовлено широким використанням відкритого коду та компонентів третіх сторін, складністю процесів інтеграції та розгортання, а також зростанням кількості учасників процесів створення ПЗ [1]. Серед найвідоміших прикладів – атаки на SolarWinds Orion та Log4j, що призвели до серйозних інцидентів інформаційної безпеки по всьому світу [2]. Тому детальне дослідження та ідентифікація процесів кібербезпеки на всіх етапах життєвого циклу ПЗ стають нагальною необхідністю для підприємств та державних установ.

Метою дослідження є розробка математичної моделі кібербезпеки ланцюга постачання програмного забезпечення, яка дозволяє ідентифікувати вразливості, оцінювати ризики та підвищувати стійкість систем до атак.

Завдання дослідження:

1. Проаналізувати існуючі загрози та вразливості в ланцюгах постачання програмного забезпечення.
2. Сформулювати математичний опис компонентів та процесів ланцюга постачання ПЗ.
3. Запропонувати модель управління ризиками на основі множинних описів.

Поняття Supply Chain

Supply Chain у сфері програмного забезпечення є складною системою, яка включає всі процеси від створення концепції продукту до його підтримки після впровадження. Це початкове проектування, написання коду, використання сторонніх бібліотек, управління репозиторіями, інтеграція окремих модулів, тестування, збірка, розгортання, оновлення та підтримка продукту. Кожен із цих етапів має

свої особливості та пов’язані ризики, наприклад, використання незахищених компонентів на етапі розробки чи вразливості в системах безперервної інтеграції та розгортання (CI/CD) [3].Кожна ланка ланцюга постачання ПЗ може бути вразливою: у відкритому чи сторонньому компоненті може бути відома або нова уразливість; обліковий запис розробника чи сервер збірки можуть бути зламані; канал оновлення може бути перехоплено або підмінено. Таким чином, компрометація будь-якого з компонентів або процесів ланцюга здатна порушити цілісність усього продукту [4]. Наприклад, у випадку атаки на SolarWinds Orion зловмисники внесли шкідливий код на етапі збірки програмного забезпечення, що пройшло до фінального продукту і було розповсюджене серед тисяч клієнтів, даючи нападникам віддалений доступ до їхніх мереж[5].

Для запобігання таким загрозам до ланцюга постачання інтегруються спеціальні процеси кібербезпеки. Під процесами кібербезпеки розуміються організаційні та технічні заходи, що реалізуються на певному етапі життєвого циклу ПЗ з метою захисту від компрометації або виявлення та нейтралізації кіберзагроз. Прикладами таких процесів є: аналіз вразливостей і ризиків постачальників на етапі розробки архітектури; запровадження процедур моніторингу вразливостей кодової бази та аналіз коду на етапі розробки; перевірка залежностей (SCA – Software Composition Analysis) під час збірки[6]

Математичний опис

Для формалізації досліджуваної системи ланцюга постачання з урахуванням кібербезпеки запропоновано множини:

$$\{I, O, S, F\}$$

де:

I – **множина входів**. До цієї множини належать вхідні коди, зовнішні бібліотеки, інструменти тестування, налаштування безпеки, облікові дані, а також фізичні чи віртуальні ресурси.

O – **множина виходів**. Це результати дій системи: готові збірки, релізи, звіти про тестування, журнал виявлених вразливостей.

S – **стан системи**. Множина станів, що описують систему на проміжних етапах розробки й тестування (стани репозиторіїв коду, конфігурації контейнерів, CI/CD-середовище, налаштування середовища розгортання, журнали безпеки тощо).

F – **функції відображення/процеси перетворення**. Множина функцій, що описують, як саме відбувається перехід від одних вхідних даних і проміжних станів до інших (наприклад, компіляція, генерація образів контейнерів, шифрування, перевірка підписів, процеси тестування).

Формули переходу та контроль безпеки

Для забезпечення безпеки в ланцюгу постачання ПЗ необхідно контролювати кожен перехідний процес між етапами розробки, тестування, складання та впровадження. У запропонованій моделі формалізовано механізм змін стану системи під впливом зовнішніх та внутрішніх факторів, що дозволяє відстежувати критичні точки ризику.

Проміжний перехід:

$$S_{t+1} = F(S_t, I_t)$$

де S_t– поточний стан на кроці t, а I_t– множина вхідних даних на кроці t.

Тут контролюється цілісність і коректність перетворення: виконується сканування вихідного коду, перевіряються підписи та сертифікати залежностей, застосовуються механізми аутентифікації та авторизації для доступу до ресурсів. У контексті кібербезпеки цей етап критично важливий для запобігання проникненню шкідливого коду та забезпечення контролю цілісності. Наприклад, на цьому кроці застосовуються такі заходи:

• Перевірка цифрових підписів і сертифікатів для підтвердження достовірності зовнішніх компонентів.

• Аналіз вразливостей відкритого коду для виявлення потенційних ризиків у використаних бібліотеках.

• Контроль доступу та аутентифікація для обмеження можливості зловмисного втручання у процес розробки.

Формування виходу:

$$O = F_{\text{final}}(S_T)$$

де T – фінальний етап процесу розробки і постачання (наприклад, версія, що публікується для кінцевих користувачів).

На цьому етапі застосовуються додаткові заходи безпеки:

• Перевірка цілісності та контрольні суми для гарантування того, що кінцевий продукт не був модифікований зловмисниками.

• Аналіз контейнерів та середовищ розгортання для виявлення прихованих загроз.

• Ретроспективний аналіз процесу розробки для відстеження можливих відхилень у ланцюгу постачання.

У систему безпеки можуть бути інтегровані додаткові обмеження:

$$C = \{\text{правила, політики, ключі, сертифікати}\}$$

що вбудовуються у функції F. Тоді перехід стану можна ускладнити:

$$S_{t+1} = F(S_t, I_t, C_t)$$

Де C_t– набір політик або правил безпеки для кроку t.

Висновки

Запропонований математичний опис забезпечує чітку структуризацію процесів кібербезпеки та дозволяє виявити критичні точки у ланцюгах постачання ПЗ. Використання цієї моделі сприяє ефективному управлінню ризиками та формуванню стійкої системи кіберзахисту. В подальших дослідженнях варто звернути увагу на розширення моделі з використанням сучасних методів аналізу даних та штучного інтелекту. Математична формалізація ланцюга постачання ПЗ через множину $\{I, O, S, F\}$ дає змогу структурувати елементи, пов'язані з безпекою, та визначити взаємозв'язки між ними. Математичний опис вказує на ті стадії, де найбільш імовірні атаки або помилки. Це дає можливість розподілити контрольні механізми (сканери вразливостей, перевірку цілісності, відповідний контроль доступу) саме у вузлових точках. Схема є масштабованою і придатною для різних середовищ – від невеликих проєктів до великих хмарних інфраструктур.

Подальші напрями досліджень:

- розробка більш детальних метрик ризику та вразливостей для кожного етапу;
- інтеграція технологій безперервного моніторингу та SIEM (Security Information and Event Management) для виявлення потенційних вразливостей;
- застосування штучного інтелекту та машинного навчання для прогнозування атак у ланцюзі постачання.

Систематизація процесів кібербезпеки у ланцюгах постачання програмного забезпечення шляхом математичного формалізму дозволяє підвищити загальний рівень захищеності ПЗ, дає можливість точніше моніторити зміни й передбачати потенційні вектори атак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Saini, Dinesh. (2012). Cyber Defense: Mathematical Modeling and Simulation. *International Journal of Applied Physics and Mathematics*. 2. 311-316.
2. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O. (Eds.) (2023). Models of socio-cyber-physical systems security. *Kharkiv*: PC TECHNOLOGY CENTER, 184. doi: http://doi.org/10.15587/978-617-7319-72-5
3. Serru, T.; Nguyen, N.; Batteux, M.; Rauzy, A. Modeling Cyberattack Propagation and Impacts on Cyber-Physical System Safety: An Experiment. *Electronics* 2023, *12*, 77. https://doi.org/10.3390/electronics12010077.
4. OX Security. *Your Guide to Software Supply Chain Security*. – 2023. – URL: https://www.ox.security/software-supply-chain-security-everything-you-need-to-know/ (accessed 06.03.2025)
5. Melara M. S., Bowman M. *What is Software Supply Chain Security?* – Proc. of ACM Workshop on Supply Chain Security (Los Angeles, 2022). – arXiv:2209.04006. – P. 1.

6. Soeiro L. et al. *Assessing the Threat Level of Software Supply Chains with the Log Model*. – Proc. of WTSC 2023. – arXiv:2311.11725. – P. 1–2.

Скіп Андрій Володимирович — аспірант кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: phd@askip.me

Науковий керівник: ***Баришев Юрій Володимирович*** — канд. техн. наук, доцент кафедри захисту інформації,факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: yuriy.baryshev@vntu.edu.ua

Skip Andrii V. — Postgraduate Student of Information Protection Department, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: phd@askip.me

Supervisor ***Baryshev Yurii V.*** — PhD. (Eng), Associate Professor of Information Protection Department, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua