isu-conference.com

ISU

INTERNATIONAL SCIENTIFIC UNITY

COLLECTION OF SCIENTIFIC PAPERS

ISSUE №51

4TH INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

SCIENCE AND INFORMATION TECHNOLOGIES IN THE MODERN WORLD

DECEMBER 24-26, 2025
ATHENS, GREECE

UDC 001(08)

Science and Information Technologies in The Modern World: Collection of Scientific Papers with Proceedings of the 4th International Scientific and Practical Conference. International Scientific Unity. December 24-26, 2025. Athens, Greece. 488 p.

ISBN 979-8-89704-987-5 (series)
DOI 10.70286/ISU-24.12.2025

The conference is included in the Academic Research Index ReserchBib International catalog of scientific conferences.

The collection of scientific papers presents the materials of the participants of the 4th International Scientific and Practical Conference "Science and Information Technologies in The Modern World" (December 24-26, 2025. Athens, Greece).

ISBN 979-8-89704-987-5

ISU
INTERNATIONAL SCIENTIFIC UNITY

Official site: https://isu-conference.com/

The final stage of training involves configuring admission control policies in orchestration environments such as Kubernetes. Students develop and implement policies that automatically block the deployment of containers lacking a valid SBOM or verified provenance. This approach allows for the practical implementation of SLSA (Supply-chain Levels for Software Artifacts) framework requirements [1], clearly demonstrating how increasing the maturity level of development processes complicates potential attacks.

Thus, integrating SBOM [2] and provenance topics into the curriculum allows for the formation of a specialist who perceives security not as a separate testing phase, but as an inherent property of the software architecture and delivery process. This aligns with modern industry standards and regulatory requirements, providing graduates with competitive advantages in the labor market.

References

1. SLSA: Supply-chain Levels for Software Artifacts. URL: https://slsa.dev (date of access: 13.12.2025).
2. The Minimum Elements for a Software Bill of Materials (SBOM) / National Telecommunications and Information Administration. Washington, DC: U.S. Department of Commerce, 2021. 19 p.

ФУНДАМЕНТАЛЬНІ ЗАСАДИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА НАПРЯМИ ЕВОЛЮЦІЇ КІБЕРЗАХИСТУ

Деркач Тетяна
к.т.н., доцент
Вербенко Ярослав
здобувач вищої освіти
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Україна

Інформаційні технології (ІТ) є фундаментальною складовою розвитку сучасного суспільства, оскільки забезпечують обробку, збереження та передавання даних, що формують основу функціонування економічних, соціальних, технічних та управлінських систем. Інформаційно-комунікаційні технології (ІКТ) інтегрують обчислювальні та телекомунікаційні засоби, створюючи єдине середовище цифрової взаємодії.

Разом із розширенням можливостей ІТ зростає і складність кіберзагроз. Апаратні уразливості, вади програмного забезпечення, помилки мережевих конфігурацій, соціальна інженерія та автоматизовані атаки на основі штучного інтелекту перетворюють інформаційний простір на одну з найважливіших площин забезпечення національної та корпоративної безпеки.

Мета дослідження – здійснити комплексний аналіз фундаментальних аспектів ІТ та окреслити сучасні виклики кібербезпеки, що виникають унаслідок розвитку цифрових технологій.

1. Фундаментальні поняття інформаційних технологій

Інформаційні технології визначаються як сукупність методів, виробничих процесів і програмно-технічних засобів, що забезпечують збір, обробку, збереження та передавання інформації. У структурі ІТ виділяють три основні складові: апаратне забезпечення, програмне забезпечення та мережеву інфраструктуру.

ІКТ виступають ширшим поняттям, що включає технології передавання інформації, засоби комунікації та сервіси для її використання. Розвиток ІКТ зумовлює трансформацію суспільства у напрямі становлення економіки знань, де інформація стає ключовим стратегічним ресурсом.

У контексті кібербезпеки особливе значення мають властивості інформації − конфіденційність, цілісність та доступність, що формують класичну тріаду CIA. Забезпечення цих властивостей є основою побудови надійних інформаційних систем.

2. Архітектура обчислювальних систем і апаратні аспекти безпеки

2.1. Архітектура фон Неймана

Класична архітектура обчислювальних систем включає арифметико-логічний пристрій, пристрій керування, пам’ять та пристрої введення/виведення. Структурна особливість − спільне зберігання даних і програм − створює низку уразливостей, зокрема можливість переповнення буфера, що використовується зловмисниками для виконання довільного коду.

2.2. Апаратні компоненти та захист

Процесори сучасних систем оснащені механізмами апаратного захисту, серед яких NX-bit (No-eXecute), що унеможливлює виконання коду в певних областях пам’яті. Оперативна пам’ять залишається вразливою до атак типу cold boot, що використовуються в комп’ютерній криміналістиці.

UEFI та Secure Boot відіграють важливу роль у захисті на етапі завантаження, запобігаючи запуску непідписаних операційних систем. Захист накопичувачів ґрунтується на методах повного шифрування дисків, що унеможливлює доступ до даних у разі фізичної компрометації пристрою.

3. Програмне забезпечення як об’єкт кіберзагроз і засіб безпеки

Системне програмне забезпечення, включно з ядром операційної системи, є ключовим елементом управління обчислювальними процесами, а його уразливості створюють передумови для загроз високого рівня.

Операційні системи Windows, Linux та macOS відрізняються особливостями архітектури захисту і частотою атак. Linux є домінуючою платформою для серверної інфраструктури та інструментів інформаційної безпеки.

Важливим аспектом безпеки є тип ліцензування програмного забезпечення. Відкриті продукти забезпечують можливість аудиту коду та виявлення бекдорів, тоді як власницькі рішення можуть містити приховані функції без можливості незалежної перевірки.

Віртуалізація дає змогу використовувати ізольоване середовище для тестування шкідливого програмного забезпечення та є ключовим інструментом у практиці кіберзахисту.

4. Мережеві технології як основа інфраструктури кіберпростору

Модель OSI та стек TCP/IP є фундаментом для аналізу мережевих взаємодій, організації маршрутизації та протоколів зв'язку. Уразливості на будь-якому рівні можуть спричинити серйозні наслідки: перехоплення трафіку, підміну DNS, атаки на маршрутизатори та сервери.

Протоколи DNS, DHCP та NAT формують критично важливу частину мережевої інфраструктури; їхня компрометація призводить до масштабних порушень доступності та цілісності даних.

Веб-технології створюють нові вектори атак, зокрема через протокол HTTP, який передає інформацію у відкритому вигляді. Перехід на HTTPS та впровадження SSL/TLS є базовою передумовою модернізації механізмів захисту даних у мережі.

5. Бази даних, великі дані та їхнє значення в кібербезпеці

Організація даних у реляційних базах ґрунтується на чіткій структурі таблиць і зв'язків, тоді як нереляційні системи NoSQL використовуються для роботи з великими потоками неструктурованих даних.

SQL Injection залишається одним із найпоширеніших типів атак, що зумовлює необхідність жорсткої фільтрації даних і використання параметризованих запитів.

Концепція Big Data охоплює характеристики обсягів, швидкості та різноманітності даних. Методи аналізу великих даних застосовуються для виявлення аномалій, прогнозування інцидентів і побудови систем моніторингу у сфері кібербезпеки.

6. Сучасні тенденції та виклики кібербезпеки

6.1. Інтернет речей (IoT)

Широке поширення IoT-пристроїв створює нові вразливості, оскільки такі пристрої часто не мають належного рівня захисту. Ботнети, утворені з IoT-пристроїв, як-от Mirai, здатні здійснювати масштабні DDoS-атаки.

6.2. Штучний інтелект

Штучний інтелект має двоїстий характер застосування: з одного боку, підсилює системи захисту, забезпечуючи виявлення аномалій, з іншого — використовується зловмисниками для оптимізації атак, генерації фішингових листів і створення глибоких фейків.

6.3. Блокчейн

Блокчейн як розподілена та незмінна структура забезпечує високий рівень захисту цілісності даних і може використовуватися для верифікації журналів подій, захисту транзакцій та побудови децентралізованих систем безпеки.

Висновки

Інформаційні технології є основою цифрової трансформації та відіграють ключову роль у розвитку сучасної інфраструктури. Водночас їхнє поширення супроводжується зростанням кіберзагроз, що потребує комплексного підходу до захисту.

Ефективна кібербезпека неможлива без глибокого розуміння архітектури комп'ютерних систем, принципів роботи програмного забезпечення, мережевих технологій, механізмів зберігання і обробки даних, а також сучасних інтелектуальних методів аналізу.

Стрімкий розвиток IT – штучного інтелекту, IoT, хмарних та блокчейн-технологій – створює як нові можливості, так і нові виклики, що потребують постійного удосконалення інструментів кіберзахисту та професійної підготовки фахівців.

Список використаних джерел

1. ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. Athens, 2023. 140 p.
2. Kurose J., Ross K. Computer Networking: A Top-Down Approach. 8th ed. Pearson, 2021. 864 p.
3. Stallings W. Operating Systems: Internals and Design Principles. 9th ed. Pearson, 2018. 944 p.
4. Данилко В.О., Деркач Т.М. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. Тези 75-ї наукової конференції професорів, викладачів, наукових працівників, аспірантів та студентів Національного університету «Полтавська політехніка імені Юрія Кондратюка». Т. 1. Полтава: Національний університет імені Юрія Кондратюка, 2023. С. 446–448.
5. Деркач Т.М., Лавренко М. Кіберпростір: аналіз загроз та методи захисту. L International scientific and practical conference «Innovative Education: Problems and Prospects of Scientific Research». Stuttgart, Germany: International Scientific Unity, 2024. С. 112–115.

VPN, TOR AND PROXY: ILLUSION OF ANONYMITY OR REAL PROTECTION?

Kyrpenko Maksym
cadet of the 2nd year
Makalish Bohdan
cadet of the 2nd year
Stoliar Mykhailo
cadet of the 2nd year
Mashukov Nikita
cadet of the 2nd year
Scientific advisor:
Kalyakin Serhii
Senior lecturer
Department of Cybercrime Counteraction
Educational and Research Institute No. 4
Kharkiv National University of Internal Affairs, Ukraine

Annotation. This study provides a comprehensive analysis of common technologies for ensuring privacy and anonymity on the internet — VPNs, the Tor network, and proxy servers — from the perspective of the actual level of protection they offer the end user. The work identifies key misconceptions associated with the