isu-conference.com

ISU

INTERNATIONAL SCIENTIFIC UNITY

COLLECTION OF SCIENTIFIC PAPERS

ISSUE №50

2ND INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

SCIENCE, TECHNOLOGY AND INDUSTRY IN THE DIGITAL AGE

DECEMBER 17-19, 2025
HAMBURG, GERMANY

UDC 001(08)

Science, Technology and Industry in the Digital Age: Collection of Scientific Papers with Proceedings of the 2nd International Scientific and Practical Conference. International Scientific Unity. December 17-19, 2025. Hamburg, Germany. 856 p.

ISBN 979-8-89704-975-2 (series)
DOI 10.70286/ISU-17.12.2025

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 2nd International Scientific and Practical Conference "Science, Technology and Industry in the Digital Age" (December 17-19, 2025. Hamburg, Germany).

ISBN 979-8-89704-975-2

ISU
INTERNATIONAL SCIENTIFIC UNITY

Список використаних джерел

1. Stonebraker, M. The Design of PostgreSQL. ACM SIGMOD Record, 2023.
2. Pavlo, A. et al. Self-Driving Database Management Systems. CACM, 2022.
3. Yu, W., & Ma, J. Machine Learning for PostgreSQL Tuning. Journal of Data Systems, 2021.
5. Momjian, B. PostgreSQL: Internals and Performance Tuning. PostgreSQL Foundation, 2020.
6. Kumar, A. Horizontal Scaling and Sharding in PostgreSQL. IEEE Transactions on Data Engineering, 2022.
7. PgTune Documentation. PostgreSQL Automatic Configuration Tool. 2024.

ІНФОРМАЦІЙНА БЕЗПЕКА В СУЧАСНОМУ ЦИФРОВОМУ СЕРЕДОВИЩІ: ЗАГРОЗИ, МЕТОДИ ЗАХИСТУ ТА МІЖНАРОДНІ СТАНДАРТИ

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

Стрімка цифровізація суспільства зумовила безпрецедентне зростання обсягів інформації, що обробляється, передається та зберігається у глобальному мережевому середовищі. Економічні процеси, державне управління, надання послуг та соціальна взаємодія дедалі більше залежать від надійності та безперервності функціонування інформаційних систем. За цих умов інформаційна безпека постає як ключовий елемент цифрової екосистеми та набуває міждисциплінарного характеру, охоплюючи технологічні, організаційні, правові та соціальні компоненти. Зростання складності кіберзагроз і уразливості критичної інфраструктури робить проблему захисту даних стратегічно важливою як для окремих організацій, так і для держави загалом. Саме тому дослідження сучасних загроз, ефективних методів протидії та міжнародних стандартів управління інформаційною безпекою є актуальним і необхідним для забезпечення стабільності цифрового середовища.

1. Сучасні загрози інформаційній безпеці.

У цифровому середовищі формується широкий спектр загроз, які постійно еволюціонують.

До ключових належать:

– шкідливе програмне забезпечення (віруси, трояни, програми-вимагачі), що становлять загрозу для цілісності та доступності даних;

– фішинг та соціальна інженерія, що спрямовані на маніпулювання користувачами з метою отримання доступу до конфіденційної інформації;

– DDoS-атаки, які дестабілізують роботу веб-сервісів та онлайн-платформ;

– використання вразливостей програмного забезпечення з метою несанкціонованого проникнення в системи;

– атаки на критичну інфраструктуру, що можуть призвести до серйозних соціальних та економічних наслідків.

Особливо небезпечними є загрози, спрямовані на державні інституції, енергетичні системи, телекомунікації та медичні заклади, адже вони можуть вплинути на функціонування суспільно важливих процесів.

2. Методи забезпечення інформаційної безпеки.

Ефективний кіберзахист ґрунтується на збалансованому застосуванні технічних, організаційних та правових заходів.

До технічних засобів належать:

– криптографічні методи захисту інформації;

– багатофакторна автентифікація;

– використання міжмережевих екранів і систем виявлення вторгнень;

– мережеве сегментування;

– регулярне оновлення та патчинг програмних компонентів.

Організаційні заходи включають управління ризиками, проведення аудитів безпеки, формування корпоративних політик доступу, а також побудову системи реагування на інциденти.

Особливе значення має людський фактор: недостатня обізнаність користувачів часто стає причиною успішних атак, тому навчання персоналу та формування культури безпечної поведінки є обов’язковими елементами комплексного захисту.

3. Міжнародні стандарти у сфері інформаційної безпеки.

Глобальна взаємодія та транснаціональний характер кібератак потребують уніфікованих підходів до управління безпекою. Найбільш поширеними стандартами є:

ISO/IEC 27000 – комплекс стандартів, що визначає принципи побудови системи управління інформаційною безпекою (ISMS) та вимоги до її сертифікації;

NIST Cybersecurity Framework – модель оцінювання та управління ризиками, що включає ідентифікацію, захист, виявлення, реагування та відновлення;

інші галузеві нормативи (наприклад, GDPR у сфері захисту персональних даних), що встановлюють вимоги до безпечної обробки інформації.

Міжнародні стандарти сприяють гармонізації практик безпеки, підвищенню кіберстійкості організацій і забезпечують можливість ефективної співпраці в умовах глобальних викликів.

Інформаційна безпека в сучасному цифровому середовищі виступає важливим чинником функціонування державних структур, бізнесу та суспільства загалом. Розмаїття та стрімка еволюція кіберзагроз потребують

комплексних, адаптивних та випереджувальних заходів захисту, що поєднують технологічні інструменти, ефективне управління ризиками та високий рівень цифрової культури. Міжнародні стандарти виступають основою для узгодження підходів до кіберзахисту та забезпечують підвищення загальної кіберстійкості на глобальному рівні. З огляду на розвиток штучного інтелекту, квантових технологій та мережі Інтернету речей, подальше вдосконалення стратегій інформаційної безпеки є необхідною умовою стабільного функціонування цифрового суспільства.

Список використаних джерел

1. GDPR − General Data Protection Regulation, EU, 2018.
2. ISO/IEC 27001:2022 Information Security Management Systems − Requirements.
3. NIST Cybersecurity Framework 2.0, National Institute of Standards and Technology, 2024.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», 2001.
5. Закон України «Про основні засади забезпечення кібербезпеки України», 2017.
6. Інформаційна безпека в інтернеті: загрози, захист, культура та право / Т. Деркач, Д. Гринюк // Research in Science, Technology and Economics : Collection of sci. papers with proceedings of the 3rd Int. sci. and pract. conf., 28-30 may, 2025. – Luxembourg, 2025. – P. 229 – 231.
7. Кіберпростор: аналіз загроз та методи захисту /Деркач Т.М., Лавренко М.//L International scientific and practical conference «Innovative Education: Problems and Prospects of Scientific Research» (December 4-6, 2024) Stuttgart, Germany. International Scientific Unity, 2024. P.112-115.

МЕТОД ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРЗАГРОЗАМ У СИСТЕМАХ АДМІНІСТРУВАННЯ

Білоусова Вероніка Олександрівна
бакалавр 122 “Комп’ютерні науки”
Селіванова Анна Віталіївна
старший викладач
Кафедра комп'ютерних наук та інформаційних систем
Державний торговельно-економічний університет, Україна

Сучасні адміністративні системи є критичною інфраструктурою для роботи організацій різного розміру, що робить їх привабливою мішенню для кіберзагроз. Ефективна безпека вимагає поєднання методів раннього виявлення та профілактичних заходів, які мінімізують ймовірність порушення та зменшують наслідки нещасних випадків. Ці дисертації систематизують ключові