Ministry of Education and Science of Ukraine
Odessa National University of Technology
Vinnytsia National Technical University
P.N. Platonov Institute of Computer Engineering, Automation, Robotics and Programming

INFORMATION TECHNOLOGIES AND AUTOMATION– 2026

PROCEEDINGS
OF THE XIX INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE



OCTOBER 29-30, 2026

Odesa

Міністерство освіти і науки України
Одеський національний технологічний університет
Інститут комп`ютерної інженерії, автоматизації, робототехніки та програмування ім.П.Н.Платонова

«ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І АВТОМАТИЗАЦІЯ – 2026»

МАТЕРІАЛИ
XIX МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ



29-30 ЖОВТНЯ 2026 р.

м.Одеса

ПРЕЗИДІЯ ТА ОРГКОМІТЕТ КОНФЕРЕНЦІЇ
ПРЕЗИДІЯ

Іванченкова Л.В. – Ректор Одеського національного технологічного університету, д.е.н., професор
Єгоров Б.В. – Радник ректора, академік НААН України, д.т.н., професор
Ольшевська О.В. – Проректор з наукової роботи та міжнародних зв'язків ОНТУ, к.т.н., доцент
Ревенюк Т.А. – Директор Навчально-наукового інституту комп`ютерної інженерії, автоматизації, робототехніки та програмування ОНТУ, к.т.н., доцент

ОРГКОМІТЕТ

Котлик С.В. – голова оргкомітету, к.т.н., доц., доцент кафедри Комп'ютерних та фізико-математичних технологій ОНТУ
Хобін В.А. – заступник голови оргкомітету, д.т.н., проф., професор кафедри Автоматизації технологічних процесів і робототехнічних систем ОНТУ
Соколова О.П. - секретар оргкомітету, старший викладач кафедри Комп'ютерних та фізико-математичних технологій ОНТУ

ЧЛЕНИ ОРГКОМІТЕТУ

Panagiotis Tzionas, prof. (Thessaloniki, Greece)
Qiang Huang, prof. (Los Angeles C.A., USA)
Yangmin Li, prof (Macao, China)
Артеменко С.В., проф., (Одеса, Україна)
Романюк О.Н., проф. (Вінниця, Україна)
Грабко В.В., проф. (Вінниця, Україна)
Жученко А.І., проф. (Київ, Україна)
Ладанюк А.П., проф. (Київ, Україна)
Лисенко В.Ф., проф. (Київ, Україна)
Любчик Л.М., проф. (Харків, Україна)
Палов І., проф. (Русе, Болгарія)
Стовкова В.Д., доц. (Тракия, Болгарія)
Суслов В., доц. (Кошалін, Польща)
Артем'єв П., проф. (Ольштин, Польща)
Судацевські В., доц. (Кишинів, Молдова)
Аманжолова С., доц. (Алмати, Казахстан)

УДК 004.01/08

Інформаційні технології і автоматизація – 2026 / Матеріали XIX міжнародної науково-практичної конференції. Одеса, 29-30 жовтня 2026 р. - Одеса, Видавництво ОНТУ, 2026 р. – 963 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

Збірник буде корисним як для фахівців і працівників фірм, зайнятих в області IT та автоматизації, так і для викладачів, магістрів і студентів вищих навчальних закладів, які навчаються за напрямами і спеціальностями програмного забезпечення, обчислювальної техніки і автоматизованих систем, прикладної математики та обробки інформації, буде корисним професіоналам з комп'ютерного моделювання та розробки комп'ютерних ігор.

Результати досліджень у збірнику представляють собою своєрідний зріз сучасного стану справ в перерахованих галузях знань, який може допомогти як фахівцям, так і студентам університетів скласти загальну картину розвитку інформаційних технологій та пов'язаних з ними питань.

Наукові праці згруповані за напрямками роботи конференції та наведені в алфавітному порядку прізвищ авторів.

Матеріали (тези доповідей) друкуються в авторській редакції. Відповідальність за якість та зміст публікацій несе автор.

Матеріали подано українською та англійською мовами.

Головний редактор збірника Сергій Котлик

©Одеський національний технологічний університет, 2026

UDC 004.01/08

Information Technologies and Automation - 2026 / Proceedings of the XIX International Scientific and Practical Conference. Odessa, October 29-30, 2026. - Odessa, ONUT Publishing House, 2026 – 963 p.

The collection includes materials of reports of conference participants, which are united by thematic areas of the conference.

The collection will be useful for professionals and employees of companies engaged in the field of IT, as well as for teachers, masters and students of higher education institutions studying in the areas and specialties of computer software and automated systems, applied mathematics and information processing, will be useful to professionals on computer modeling and development of computer games.

The results of research in the collection are a kind of slice of the current state of affairs in these areas of knowledge, which can help both professionals and university students to get a general picture of the development of information technology and related issues.

Scientific papers are grouped by areas of the conference and are listed in alphabetical order of the authors.

Materials (abstracts) are published in the author's edition. The author is responsible for the quality and content of publications.

Materials are submitted in Ukrainian and English.

Editor-in-Chief of the collection Sergii Kotlyk.

© Odessa national university of technology 2026

ПРОБЛЕМАТИКА КОНФЕРЕНЦІЇ

- *МАТЕМАТИЧНЕ І КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ СКЛАДНИХ ПРОЦЕСІВ*
- *УПРАВЛІННЯ, ОБРОБКА ТА ЗАХИСТ ІНФОРМАЦІЇ*
- *АВТОМАТИЗАЦІЯ ТА УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ*
- *НОВІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ*
- *ПРОЕКТУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНИХ КОМПЛЕКСІВ*
- *КОМП'ЮТЕРНІ ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ ТА ТЕХНОЛОГІЇ*
- *ШТУЧНИЙ ІНТЕЛЕКТ І АВТОМАТИЗАЦІЯ РОБОТОТЕХНІЧНИХ СИСТЕМ*
- *КОМП'ЮТЕРНІ ІГРИ І WEB-ДИЗАЙН*
- *БІБЛІОМЕТРИКА. ІНФОРМАТИЗАЦІЯ НАВЧАЛЬНОГО, НАУКОВОГО, ДОСЛІДНОГО ПРОЦЕСІВ*
- *ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В МЕДИЦИНІ*
- *3D МОДЕЛЮВАННЯ ТА 3D ДРУК*

PROBLEMS OF THE CONFERENCE

- *MATHEMATICAL AND COMPUTER SIMULATION OF COMPLEX PROCESSES*
- *MANAGEMENT, PROCESSING AND PROTECTION OF INFORMATION*
- *AUTOMATION AND MANAGEMENT OF TECHNOLOGICAL PROCESSES*
- *NEW INFORMATION TECHNOLOGIES IN EDUCATION*
- *DESIGN OF INFORMATION SYSTEMS AND SOFTWARE COMPLEXES*
- *COMPUTER TELECOMMUNICATION NETWORKS AND TECHNOLOGIES*
- *ARTIFICIAL INTELLIGENCE AND AUTOMATION OF ROBOTIC SYSTEMS*
- *COMPUTER GAMES AND WEB DESIGN*
- *BIBLIOMETRIC. INFORMATIZATION OF EDUCATIONAL, SCIENTIFIC, RESEARCH PROCESSES*
- *INFORMATION TECHNOLOGIES IN MEDICINE*
- *3D MODELING AND 3D PRINTING*

порушення властивостей інформації. Таке тлумачення узгоджується з Національним планом реагування на кіберінциденти, кібератаки та кіберзагрози.

Список використаної літератури

1. В. В. Мохор, Я. Ю. Дорогий, В. С. Ракович, В. В. Цуркан, “Погляд на парадигму повідомляння про події кібербезпеки об’єктів критичної інфраструктури”, *на VIII міжнародної науково-практичної конференції Перспективні напрями захисту інформації*, Одеса, 2026. с. 104–106.

2. International Organization for Standardization. (2023, Febr. 13). *ISO/IEC 27035-2, Information technology. Information security incident management. Part 2: Guidelines to plan and prepare for incident response*. [Online]. Available: https://www.iso.org/standard/78974.html.

3. Кабінет Міністрів України. (2025, Листоп. 26). *Постанова Кабінету міністрів України № 1533, Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#n12.

УДК 004.89

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ІНКЛЮЗИВНИХ ЦИФРОВИХ СИСТЕМАХ

В. Недашківська (valeriia.nedashkivska@m.hneu.edu.ua)
Н. Бринза (natalia.brynza@hneu.net)
Харківський національний економічний університет імені Семена Кузнеця

У роботі досліджено сучасні підходи до забезпечення кібербезпеки та захисту персональних даних в інклюзивних цифрових системах. Розглянуто основні загрози, пов’язані з використанням допоміжних технологій та вебплатформ, а також методи їх нейтралізації на основі концепцій Defense in Depth, Privacy by Design і Zero Trust Architecture. Проаналізовано застосування адаптивної багатофакторної автентифікації, криптографічних протоколів TLS 1.3 та AES-256, поведінкової біометрії, WAF-систем і технологій Blockchain для захисту чутливих даних користувачів. Особливу увагу приділено проблемам доступності інтерфейсів безпеки відповідно до стандартів WCAG 2.2 та ролі цифрової грамотності у протидії соціальній інженерії. Визначено перспективи розвитку інклюзивних цифрових середовищ із використанням штучного інтелекту та автоматизованих систем реагування на інциденти.

Сучасний етап розвитку цифрової освіти та соціальної сфери потребує інклюзивних рішень, які базуються на принципах універсального дизайну та рівного доступу. Інклюзивна цифрова система – це складний програмно-апаратний комплекс, який має бути однаково функціональним для користувачів із сенсорними, когнітивними чи моторними порушеннями. Однак розширення точок доступу та активне впровадження допоміжних технологій, таких як програми екранного доступу Screen Readers або системи голосового керування Voice Control, створює специфічні вектори атак. Захист такої системи не може бути фрагментарним; він має базуватися на стратегії ешелонованої оборони Defense in Depth, де кожен рівень – від фізичної інфраструктури сервера до інтерфейсу кінцевого користувача – має власні механізми стримування загроз.

Одним із ключових викликів є забезпечення конфіденційності даних про особливі освітні потреби або стан здоров'я користувачів, які система збирає для автоматичної адаптації контенту. Такі дані належать до особливої категорії, і їх компрометація може призвести до серйозних етичних та юридичних наслідків. Тому архітектура інклюзивної системи повинна будуватися на засадах Privacy by Design. Це означає, що мінімізація збору даних інтегрується в систему за замовчуванням: платформа має знати параметри необхідної адаптації інтерфейсу, але не обов'язково зберігати конкретний діагноз чи медичні висновки користувача. Це досягається шляхом використання метаданих про вподобання користувача, які не пов'язані безпосередньо з його особою, що дозволяє системі бути гнучкою, залишаючись при цьому анонімною на рівні обробки чутливої інформації.

Традиційні методи захисту, зокрема складні текстові паролі, часто стають бар'єром для людей з дислексією або порушеннями дрібної моторики. В інклюзивних системах пріоритет надається адаптивній багатофакторній автентифікації (MFA). Використання стандартів FIDO2 та апаратних ключів безпеки дозволяє користувачам входити в систему за допомогою одного дотику або наближення пристрою, що є значно надійнішим за SMS-коди, які вразливі до перехоплення через атаки типу SIM-swapping. Біометрична ідентифікація, така як FaceID або сканування відбитка пальця через протокол WebAuthn, є зручною альтернативою, що вимагає суворого захисту біометричних шаблонів. Система має оперувати виключно математичними хеш-функціями біометрії, що унеможливлює відновлення персональних даних у разі несанкціонованого доступу до бази даних. Важливо впроваджувати поведінкову біометрію, яка аналізує динаміку натискання клавіш або рухи миші, що дозволяє системі розпізнати власника акаунта за його унікальною моторикою, не створюючи додаткових когнітивних навантажень.

Для забезпечення цілісності інформації під час її передачі обов'язковим є використання сучасних криптографічних протоколів. Протокол TLS 1.3 гарантує шифрування каналу зв'язку, мінімізуючи затримки під час встановлення з'єднання, що критично для користувачів із асистивними технологіями, які чутливі до швидкості відгуку інтерфейсу. Збережені дані Data-at-Rest мають захищатися алгоритмами симетричного шифрування стандарту AES-256. Додатково доцільно впроваджувати технології гомоморфного шифрування, які дозволяють виконувати аналітичні операції над зашифрованими масивами даних (наприклад, підрахунок статистики відвідуваності) без необхідності їх попереднього розшифрування, що фактично нівелює ризик витоку в процесі обробки. Це особливо важливо для великих освітніх платформ, де обробляються масиви статистичних даних про прогрес тисяч користувачів, і кожна операція розшифрування створює потенційне вікно вразливості для зловмисників.

Оскільки більшість інклюзивних систем реалізовані як вебплатформи, вони піддаються ризикам, описаним у переліку OWASP Top 10. Захист від SQL-ін'єкцій, які спрямовані на викрадення баз даних, та атак типу Cross-Site Scripting (XSS) забезпечується впровадженням міжмережевих екранів прикладного рівня (WAF). Це інтелектуальні системи, що аналізують вхідний трафік у реальному часі та блокують шкідливі запити на основі сигнатурного та поведінкового аналізу. Окрім цього, критично важливим є регулярне проведення аудитів безпеки та тестів на проникнення (Pentesting), що дозволяє виявляти вразливості в сторонніх модулях та плагінах, які часто використовуються для забезпечення інклюзивності, таких як віджети синтезу мовлення або екранні лупи. Необхідно враховувати, що будь-який сторонній скрипт, інтегрований у систему для покращення доступності, може стати «чорним ходом» для хакерів, якщо він не проходить належної перевірки коду на відповідність безпековим стандартам.

Управління доступом у сучасних системах переходить від статичних моделей до архітектури нульової довіри (Zero Trust Architecture). Вона базується на принципі постійної верифікації кожного запиту. Кожна дія користувача перевіряється за сукупністю атрибутів: ідентичність особи, стан безпеки пристрою, геопозиція та типовість поведінки. Модель ABAC (Attribute-Based Access Control) дозволяє гнучко налаштовувати права, забезпечуючи доступ до конфіденційних розділів системи лише за умови успішного проходження всіх етапів перевірки, незалежно від того, чи перебуває користувач у внутрішній мережі установи, чи підключається через публічну мережу. Такий підхід мінімізує збитки від скомпрометованих облікових записів, оскільки навіть у разі крадіжки логіна та пароля зловмисник не зможе отримати повний доступ до системи без відповідності іншим критеріям безпеки, таким як перевірений пристрій або географічна прив'язка. На рис. 1 представлено узагальнену архітектуру кіберзахисту інклюзивної цифрової системи.

Найслабшою ланкою в системі кіберзахисту залишається людський фактор. В інклюзивному середовищі ризики соціальної інженерії зростають, оскільки зловмисники можуть використовувати складність технічних налаштувань для маніпуляцій під виглядом «технічної допомоги». Тому інтерфейси налаштування приватності повинні відповідати стандартам WCAG 2.2, бути максимально зрозумілими та доступними для сприйняття. Кожна зміна параметрів безпеки має супроводжуватися чіткими поясненнями та зворотним зв'язком, щоб користувач розумів рівень захищеності свого профілю. Прозорість політик конфіденційності, викладених простою мовою (Plain Language), сприяє підвищенню цифрової грамотності користувачів і

формуванню культури безпечної поведінки в мережі, що є першим ешелоном оборони проти фішингу та шахрайства.

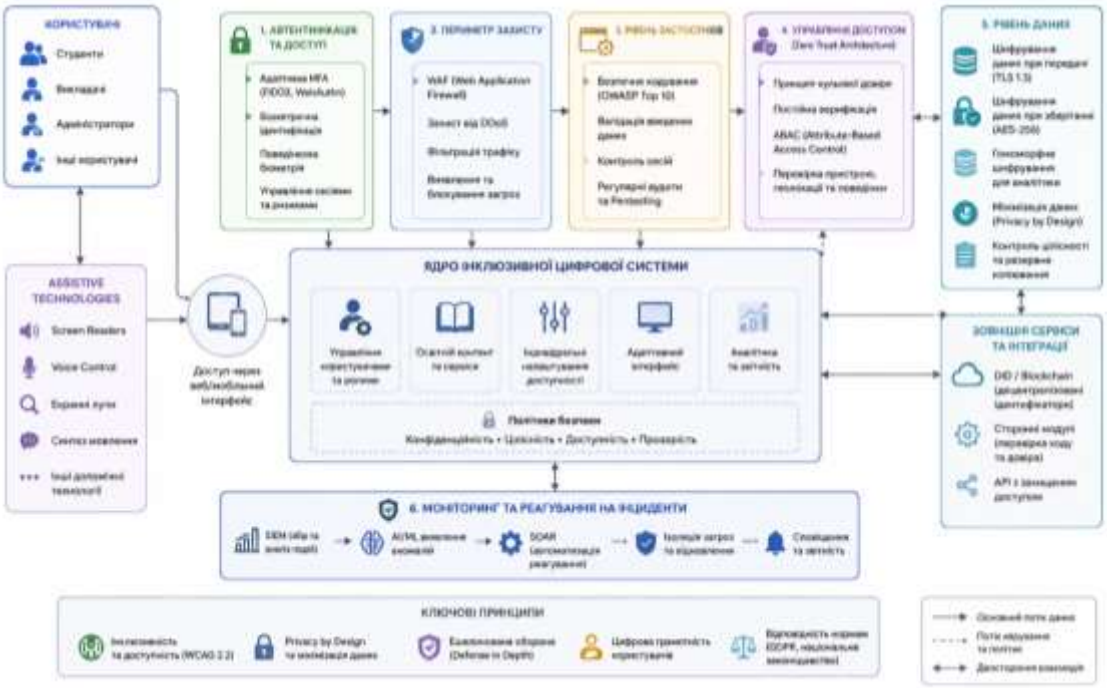


Рис. 1 – Архітектура кіберзахисту інклюзивної цифрової системи

Перспективним напрямком розвитку є використання технології Blockchain для створення децентралізованих ідентифікаторів (DID). Це дозволяє користувачеві самостійно контролювати свої персональні дані та надавати системі лише обмежений, тимчасовий доступ до них через смартконтракти. Поєднання штучного інтелекту для виявлення аномальної активності та децентралізованих методів зберігання інформації дозволить створити по-справжньому захищене та інклюзивне цифрове середовище. Важливо також впроваджувати автоматизовані системи реагування на інциденти (SOAR), які здатні миттєво ізолювати підозрілий сегмент мережі або заблокувати обліковий запис у разі виявлення ознак масованої атаки, що значно скорочує час реагування та зменшує потенційні втрати даних.

Безпека інклюзивних систем – це безперервний процес вдосконалення технічних засобів та підвищення свідомості кожного учасника цифрової екосистеми.

Список використаної літератури

1. Web Content Accessibility Guidelines (WCAG) 2.2 [Електронний ресурс]. – Режим доступу: https://www.w3.org/TR/WCAG22/

2. OWASP Top 10:2025 [Електронний ресурс]. – Режим доступу: https://owasp.org/Top10/2025/

3. Що таке FIDO2? [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-fido2

4. The Transport Layer Security (TLS) Protocol Version 1.3 [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc8446

5. Decentralized Identifiers (DIDs) v1.1 [Електронний ресурс]. – Режим доступу: https://www.w3.org/TR/did-1.1/

6. What is Zero Trust architecture? [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/en-us/security/business/security-101/what-is-zero-trust-architecture

7. Understanding Homomorphic Encryption: Enabling Secure Data Processing and Addressing Practical Challenges [Електронний ресурс]. – Режим доступу: https://medium.com/@aditya-sunjava/understanding-homomorphic-encryption-enabling-secure-data-processing-and-addressing-practical-94d78a0af1aa.