НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

**28 листопада 2025 року**

# КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

**МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**Національний університет «Одеська юридична академія»**
**Факультет кібербезпеки та інформаційних технологій**
**Кафедра кібербезпеки**

# КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

**МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

**28 листопада 2025 року, м. Одеса**

Одеса, 2025

**MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE**
**National University «Odesa Law Academy»**
**Faculty of Cybersecurity and Information Technologies**
**Department of Cybersecurity**

# CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

**MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE**

**November 28, 2025, Odesa**

Odesa, 2025

УДК 004.056

**Відповідальній редактор:**

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

## Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

**VI Міжнародна науково-практична конференція**

# «Кібербезпека в сучасному світі: актуальні виклики»

**28 листопада 2025 року**

**ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:**

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

**VI International Scientific and Practical Conference**

# «Cybersecurity in today's world: actual challenges»

**28 November 2025 year**

**THEMATIC DIRECTIONS OF THE CONFERENCE:**

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

вийшли з 2018 року, поступово змінювали підхід цілої індустрії до створення нових мультфільмів. Люди по всьому світу зараз цікавляться оригінальною і експериментальною анімацією, яка, найчастіше, поєднує 3D і 2D, створюючи унікальний художній стиль та розповідає захопливу історію, зрозумілу глядачам зі всього світу. Для того щоб індустрія анімації в Україні досягла подібного рівня, народ і влада України повинні надати фінансові та юридичні можливості незалежним студіям для створення власних анімаційних проектів, стимулюючи добросовісну конкуренцію між усіма студіями.

**Список використаних джерел**:

1. Олексійчук К. О. Розробка 3D моделі персонажа для мультфільму. – 2025.
2. Гребенюк І. В., Басараба В. М., Левицька Р. Р. Сучасні тенденції в графічному дизайні: взаємодія естетики та технологій. – 2025.
3. Кобзев І., Курбін П. Створення 3d product animation для промоції продукту. – 2025.
4. Тимощук Н. М. ПЕРЕКЛАДАЦЬКІ РІШЕННЯ В АНІМАЦІЙНОМУ ФІЛЬМІ «МАВКА. ЛІСОВА ПІСНЯ» //Наукові записки. Серія: Філологічні науки. – 2025. – №. 212. – С. 242-246.

**Ключові слова:** генеративний ШІ.
**Keywords:** generative AI.

## ОСОБЛИВОСТІ ЗАХОДІВ КІБЕРБЕЗПЕКИ У РЕСТОРАННІЙ СФЕРІ

***Разінкін Нікіта***

*аспірант кафедри статистики та ММЕ Одеського національного економічного університету*

***Нгуен Фиок Бао Шон***

*студент факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»*

У сфері ресторанного бізнесу, яка є невід'ємною частиною індустрії гостинності, заходи кібербезпеки набувають особливого значення через швидку цифровізацію процесів, що включає обробку персональних даних клієнтів, управління системами точок продажу та інтеграцію з онлайн-платформами для замовлень і доставки. Така цифрова трансформація, з одного боку, сприяє підвищенню ефективності та персоналізації послуг, а з іншого – створює численні вразливості, які експлуатуються кіберзлочинцями для отримання доступу до конфіденційної інформації, такої як дані кредитних карток, адреси електронної пошти та контактні номери. Як науковець, що спеціалізується на аналізі ризиків у сфері послуг, я підкреслюю, що ресторанний сектор стикається з унікальними викликами, пов'язаними з

високим оборотом персоналу, обмеженими ресурсами на впровадження складних систем захисту та залежністю від постачальників третіх сторін, що часто призводить до ланцюгових порушень. Згідно з аналізом, проведеним у контексті стійких систем послуг, ключовими зацікавленими сторонами є клієнти, співробітники, постачальники, акціонери, регулятори, конкуренти та медіа, кожен з яких по-різному впливає на рівень ризику та відповідальності за його мінімізацію. Наприклад, регулятори відіграють домінуючу роль у встановленні норм, тоді як клієнти та співробітники є найбільш залежними від ефективності заходів захисту [1].

Серед основних кіберзагроз у ресторанній сфері виділяються фішингові атаки, порушення даних, програми-вимагачі, атаки на відмову в обслуговуванні та системні вразливості, які часто кореняться в людському факторі, застарілих технологіях та слабких ланцюгах постачання. Фішинг, як одна з найпоширеніших тактик, передбачає обман співробітників або клієнтів через фальшиві електронні листи чи повідомлення, що призводить до витоку даних або встановлення шкідливого ПЗ, і є причиною багатьох подальших порушень, таких як крадіжка даних кредитних карток у системах POS. Порушення даних, у свою чергу, являють собою несанкціонований доступ до конфіденційної інформації, як це сталося в випадку з великими мережами ресторанів, де витік стосувався мільйонів клієнтів, включаючи імена, номери соціального страхування та фінансові деталі, що спричинило не лише фінансові втрати, але й втрату довіри. Програми-вимагачі блокують доступ до критичних систем, таких як бази даних замовлень чи інвентарю, вимагаючи викуп, і часто призводять до тимчасового закриття закладів, як у випадку з майже 300 ресторанами у Великобританії, де атака спричинила хаос у операціях. Атаки DoS перевантажують сервери, роблячи сайти чи системи замовлень недоступними, що особливо шкідливо для ресторанів з онлайн-присутністю, тоді як системні вразливості, такі як незахищені Wi-Fi чи неоновлені POS-термінали, служать точками входу для хакерів, експлуатуючи слабкості в апаратному чи програмному забезпеченні [1,2].

Конкретні приклади порушень у ресторанній сфері ілюструють серйозність проблеми та необхідність адаптованих заходів. Наприклад, у 2015 році атака на мережу Hilton торкнулася POS-систем у ресторанах і магазинах готелів, викравши дані 350 тисяч кредитних карток, включаючи імена, коди безпеки та терміни дії, що призвело до штрафу в 700 тисяч доларів через затримку в реагуванні. Аналогічно, порушення в Wyndham Hotels з 2008 по 2010 рік зачепили понад 619 тисяч записів клієнтів, включаючи кредитні картки, спричинивши шахрайство на суму понад 1,6 мільйона доларів і значні юридичні витрати. У ресторанному сегменті, як у випадку з великими мережами швидкого харчування, атаки часто починаються з несанкціонованого доступу до електронної пошти співробітників, що дозволяє

хакерам збирати облікові дані та проникати глибше в мережу, експлуатуючи високий оборот персоналу та низьку обізнаність з кібербезпеки. Ці інциденти підкреслюють, що наслідки включають не лише безпосередні фінансові втрати, але й репутаційні збитки, судові позови та операційні перебої, які можуть тривати дні чи тижні, особливо в умовах, коли близько 80% транзакцій у ресторанах є цифровими [2,3].

Для ефективного протистояння цим загрозам у ресторанній сфері необхідне впровадження комплексних заходів, що охоплюють як технічні, так і організаційні аспекти. Серед ключових практик – регулярне навчання персоналу з розпізнавання фішингу та соціальної інженерії, оскільки людський фактор є причиною більшості порушень, і це вимагає постійних сесій, враховуючи високий оборот кадрів у швидкому обслуговуванні. Важливим є впровадження багатофакторної аутентифікації для всіх систем, сильних політик паролів, що включають комбінацію символів, цифр і букв, та обмеження доступу до чутливої інформації на основі ролей співробітників, аби мінімізувати внутрішні загрози від недбалості чи зловмисності. На технічному рівні рекомендується проводити регулярні оцінки вразливостей, оновлення програмного забезпечення та апаратного забезпечення, шифрування даних у POS-системах від кінця до кінця, щоб запобігти перехопленню під час передачі, а також розділення гостьових Wi-Fi мереж від внутрішніх для уникнення витоків через незахищені з'єднання. Крім того, створення планів реагування на інциденти, що включають крос-функціональні команди з IT-спеціалістів, керівництва та юристів, дозволяє швидко локалізувати порушення, повідомляти зацікавлених сторін і відновлювати операції, зменшуючи витрати на відновлення. Управління ризиками третіх сторін, такими як постачальники доставки чи платформи бронювання, вимагає ретельної перевірки їхніх стандартів безпеки та регулярних аудитів, оскільки порушення в ланцюгу постачання, як у випадку з Marriott-Starwood, можуть поширитися на весь бізнес [3,4,5].

Додатково, для стійкості ресторанного бізнесу до кіберзагроз варто впроваджувати резервне копіювання даних у хмарних сховищах, відокремлених від основної мережі, аби швидко відновлюватися після атак вимагачів, та використовувати інструменти моніторингу в реальному часі для виявлення аномалій, що скорочує час перебування зловмисників у системі, який у цій галузі може перевищувати рік. З точки зору стійких систем, аналіз за допомогою методів, таких як PFSs-MACTOR, показує, що посилення регуляторних норм, таких як PCI DSS для платежів чи GDPR для даних, є критичним для координації зусиль усіх стейкхолдерів, де регулятори домінують у встановленні стандартів, а співробітники та клієнти потребують підвищення обізнаності для протидії фішингу як кореневій причині багатьох ризиків. У контексті швидкого харчування та роздрібної торгівлі продуктами

харчування, де цифрова взаємодія з клієнтами через додатки лояльності та кіоски самообслуговування є нормою, акцент на шифруванні чутливих даних і регулярних тестах безпеки стає невід'ємним для запобігання хаосу в операціях [1,4].

Нарешті, ефективність заходів кібербезпеки в ресторанній сфері залежить від створення культури безпеки, де керівництво з верхівки до низу інтегрує захист як щоденну практику, поєднуючи з інноваціями, такими як штучний інтелект для виявлення аномалій і прогнозування загроз. Це не лише мінімізує фінансові та репутаційні втрати, але й сприяє стійкому розвитку індустрії, забезпечуючи довіру клієнтів у цифрову епоху.

### Список використаних джерел

1. Karadayi-Usta S. Cybersecurity Risks Analysis in the Hospitality Industry: A Stakeholder Perspective on Sustainable Service Systems. *Systems.* 2024. №12(10):397. DOI: https://doi.org/10.3390/systems12100397
2. Elgan M. The rising threat of cyberattacks in the restaurant industry. IBM. URL: https://www.ibm.com/think/news/rising-threat-cyberattacks-restaurant-industry (дата звернення: 30.10.2025).
3. Chin K. Cybersecurity in the Hospitality Industry: Challenges and Solutions. UpGuard. URL: https://www.upguard.com/blog/cybersecurity-in-the-hospitality-industry (дата звернення: 30.10.2025).
4. Cybersecurity Best Practices for Food Retailers and QSR. NSF. URL: https://www.nsf.org/knowledge-library/cybersecurity-best-practices-for-food-retailers-and-qsr (дата звернення: 30.10.2025).
5. Pollak N. Cybersecurity for restaurants: 7 common risks and how to avoid them. Cloud Kitchens. URL: https://cloudkitchens.com/blog/cybersecurity-for-restaurants/ (дата звернення: 30.10.2025).

**Ключові слова:** кібербезпека, POS-системи, фішингові атаки, багатофакторна аутентифікація, шифрування даних, управління ризиками, цифровізація.
**Keywords:** cybersecurity, POS systems, phishing attacks, multi-factor authentication, data encryption, risk management, digitalization.

## СИСТЕМНИЙ АНАЛІЗ ТА ОПТИМІЗАЦІЯ ЕФЕКТИВНОСТІ ВЕБПОРТАЛУ НА ОСНОВІ ПОВЕДІНКИ КОРИСТУВАЧА

***Куклінова Софія***
*студентка факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»*

У сучасних реаліях вебпортали виступають не лише засобом представлення інформації, а й ключовим інструментом інформаційного обміну, комунікації та взаємодії між користувачами і цифровими сервісами. Від

## Секція 3. УПРАВЛІНСЬКІ, СОЦІАЛЬНІ ТА ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ.....211

ПЕРСПЕКТИВИ СТВОРЕННЯ КЛАСТЕРУ КІБЕРБЕЗПЕКИ В УКРАЇНІ ..... 211
*Горбаченко Станіслав*
*Саврацький Олександр*

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ТОКСИЧНОГО КОНТЕНТУ ПРИ СПІЛКУВАННІ УКРАЇНСЬКОЮ МОВОЮ ..... 213
*Гура Володимир*
*Касян Павло*

ГЕНЕЗИС РОЗВИТКУ 3D-ТЕХНОЛОГІЙ У МОДЕЛЮВАННІ ТА АНІМАЦІЇ ..... 218
*Задерейко Олександр*
*Тимофєєв Михайло*

ОСОБЛИВОСТІ ЗАХОДІВ КІБЕРБЕЗПЕКИ У РЕСТОРАННІЙ СФЕРІ..... 221
*Разінкін Нікіта*
*Нгуен Фиок Бао Шон*

СИСТЕМНИЙ АНАЛІЗ ТА ОПТИМІЗАЦІЯ ЕФЕКТИВНОСТІ ВЕБПОРТАЛУ НА ОСНОВІ ПОВЕДІНКИ КОРИСТУВАЧА..... 228
*Куклінова Софія*

ANALYSIS AND MODELING OF THE PLAYER'S EMOTIONAL STATES IN ADAPTIVE GAME DESIGN SYSTEMS ..... 230
*Chepurna Olena*
*Shliakhtytskyi Dmytro*

ДОСЛІДЖЕННЯ МЕТОДІВ АДАПТАЦІЇ ІНТЕРФЕЙСІВ ДЛЯ КОРИСТУВАЧІВ З КОГНІТИВНИМИ ПОРУШЕННЯМИ..... 2360
*Гура Володимир*
*Вдовін Олександр*

КОМУНІКАЦІЙНІ СТРАТЕГІЇ ПРОТИДІЇ РЕПОСТАМ І «ДЗЕРКАЛАМ» МУЛЬТИМЕДІЙНОГО КОНТЕНТУ: ВЗАЄМОДІЯ З ПЛАТФОРМАМИ ТА СПІЛЬНОТАМИ ..... 239
*Овчинников Микола*

ПЛАТФОРМЕНА ЕКОНОМІКА: МОЖЛИВОСТІ ТА ВИКЛИКИ..... 241
*Маріна Аліна*

НМІ ЯК ЧИННИК ЦИФРОВОЇ ЕВОЛЮЦІЇ УПРАВЛІНСЬКИХ ПРАКТИК ..... 245
*Кочубинська Юлія*

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОДУКТИВНОСТІ ДЕКЛАРАТИВНОГО ТА ІМПЕРАТИВНОГО ПІДХОДІВ ДО ПОБУДОВИ КОРИСТУВАЦЬКИХ ІНТЕРФЕЙСІВ МОБІЛЬНИХ ЗАСТОСУНКІВ..... 2475
*Земан Артур*