ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС
Матеріали Міжнародної науково-практичної конференції
2

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

Одеса
2025

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 16.05.2025 р.)

За загальною редакцією ***С. В. Ківалова***

Є 24 **Європейські орієнтири розвитку України: нові виміри у воєнний час** : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 16 травня 2025 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2025. – Т. 2. – 716 с.
ISBN 978-617-8430-61-0

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири України: нові виміри у воєнний час» містять результати наукових досліджень і практичних напрацювань вчених, фахівців і військовослужбовців, здійснені в умовах повномасштабної війни. У збірнику представлено як теоретичні, так і емпіричні дослідження у галузях філософії, загальної теорії держави і права, історії права, сучасних соціально-політичних процесів, соціології та психології.

Особливу увагу приділено аналізу загроз національній безпеці в конституційному, міжнародному та європейському правовому контекстах, а також питанням трудового, соціального, земельного, аграрного та екологічного права. Окремі розділи присвячено функціонуванню економіки та підприємництва в умовах євроінтеграції.

У збірнику також розглянуто проблематику цифрової трансформації, захисту інформації та кібербезпеки в умовах воєнного часу, методику викладання іноземних мов, перекладознавство, лінгвістику і журналістику. Висвітлено наукові здобутки в адміністративному, фінансовому, морському та митному праві, реформуванні судової системи, діяльності прокуратури, правоохоронних органів та адвокатури. Окремо проаналізовано питання кримінального права, кримінального процесу, кримінології, криміналістики, судової експертизи, медико-психологічного забезпечення правосуддя, а також аспекти цивільного, сімейного, господарського права, інтелектуальної власності та патентного судочинства. Розглянуто також актуальні питання діяльності бібліотек у закладах вищої освіти та фізичної підготовки здобувачів вищої освіти.

Збірник адресовано науковцям, викладачам, здобувачам вищої освіти, а також практикам у галузях права, економіки, соціології, політології, психології, філології, журналістики та кібербезпеки.

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)

Відповідальний за випуск ***М. Р. Аракелян***

ISBN 978-617-8430-61-0

© НУ «Одеська юридична академія, 2025
© Автори статей, 2025

СЕКЦІЯ 22. ІНФОРМАТИЗАЦІЯ ТА ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА В ЕПОХУ СТРІМКОГО РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Логінова Наталія Іванівна
ПОРІВНЯННЯ БІБЛІОТЕК PYTHONДЛЯ КЕРУВАННЯ БАЗАМИ ДАНИХ 486

Гура Володимир Ігорович
КОМПЛЕКСНИЙ АНАЛІЗ КІБЕРЗАГРОЗ В ІНТЕЛЕКТУАЛЬНИХ ЕНЕРГОСИСТЕМАХ 489

Задерейко Олександр Владиславович
АНАЛІЗ ПРОБЛЕМАТИКИ ФОРМУВАННЯ РЕЛЕВАНТНОСТІ ПОШУКУ НАУКОВОЇ ІНФОРМАЦІЇ 493

Куклінова Тетяна Вікторівна, Куклінова Софія Іванівна
ШТУЧНИЙ ІНТЕЛЕКТ І ЗЕЛЕНИЙ ВОДЕНЬ ДЛЯ СТАЛОГО РОЗВИТКУ 497

Лобода Юлія Геннадіївна
ЕФЕКТИВНІ ІНСТРУМЕНТИ ТА ПІДХОДИ ВІЗУАЛІЗАЦІЇ ДАНИХ В АНАЛІТИЧНОМУ ПРОЦЕСІ 501

Манаков Сергій Юрійович
ПАТЕРНИ БЕЗСЕРВЕРНОЇ АРХІТЕКТУРИ 504

Трофименко Олена Григорівна
ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА КОНКУРЕНТОСПРОМОЖНІСТЬ В ІТ 506

Чанишев Рашид Ібрагімович
PROTECTEU – НОВА ВНУТРІШНЯ СТРАТЕГІЯ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ 510

Чикунов Павло Олександрович
ПРОЄКТУВАННЯ ВЕБОРІЄНТОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ УНІВЕРСАЛЬНОЇ ПЛАТФОРМИ WINDOWS 513

Щербина Юрій Володимирович
АНАЛІЗ ЕФЕКТИВНОСТІ ПРОГРАМНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ . . . 517

Дика Анастасія Іванівна
ЗАСТОСУВАННЯ NLP-МЕТОДІВ ДЛЯ ВИЯВЛЕННЯ XSS-АТАК 520

Грезіна Олена Миколаївна
ЗАСТОСУВАННЯ СИСТЕМНОГО АНАЛІЗУ ДЛЯ ІНТЕГРАЦІЇ РІЗНИХ БАЗ ДАНИХ В ВЕБЗАСТОСУНКАХ 523

Соловйов Артем Сергійович
ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ КІБЕРБЕЗПЕКИ ОСОБИ В ЦИФРОВУ ЕПОХУ 526

Толокнов Анатолій Арнольдович
ПРОЦЕДУРНА ГЕНЕРАЦІЯ У ВІДЕОІГРАХ:ОГЛЯД МЕТОДІВ, ЗАСТОСУВАНЬ ТА ПЕРСПЕКТИВ 529

СЕКЦІЯ 23. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

Горбаченко Станіслав Анатолійович
ЗАСТОСУВАННЯ МЕТОДОЛОГІЇ SCRUM У ВИРІШЕННІ ЗАДАЧ КІБЕРБЕЗПЕКИ 533

Соколов Артем Вікторович, Радуш Володимир Вячеславович
МЕТОД НЕДВІЙКОВОГО АФІННОГО ПЕРЕТВОРЕННЯ ДЛЯ ПІДВИЩЕННЯ КРИПТОГРАФІЧНОЇ ЯКОСТІ S-БЛОКІВ 536

Ахаметьєва Ганна Валеріївна, Овчинников Микола Юрійович
ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ШИРОКОСМУГОВОГО ТА ФАЗОВОГО КОДУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ В АУДІОСИГНАЛІ 539

Бойко Віктор Дмитрович
ПРОБЛЕМИ ШВИДКОГО РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ У ВЕБ-СЕРВЕРАХ СЕРЕДНЬОГО ТА НИЗЬКОГО РІВНЯ 543

Соловйов Артем Сергійович
Національний університет «Одеська юридична академія»,
асистент кафедри інформаційних технологій

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ КІБЕРБЕЗПЕКИ ОСОБИ В ЦИФРОВУ ЕПОХУ

У сучасному світі стрімкий розвиток цифрових технологій супроводжується зростанням загроз у кіберпросторі, що безпосередньо впливає на безпеку особистості, суспільства та держави. Особливої актуальності набуває питання захисту персональних даних – інформації, що стосується конкретної особи та використовується у найрізноманітніших сферах: від соціальних мереж до державного управління. Неналежний рівень захисту цих даних створює реальні ризики втручання в особисте життя, фінансових втрат, шахрайства, а також становить загрозу інформаційній безпеці держави.

Персональні дані – це будь-яка інформація, яка стосується фізичної особи та дозволяє прямо або опосередковано її ідентифікувати. В умовах цифровізації суспільства, обсяг таких даних постійно зростає. Сюди входять: ім'я, прізвище, дата народження, адреса, номер телефону, електронна пошта, ІПН, біометричні та медичні дані, дані про місцезнаходження, історія покупок, дії в інтернеті, тощо [1].

У сучасному цифровому середовищі персональні дані є цінним ресурсом. Їх активно збирають і використовують приватні компанії для комерційних цілей (таргетинг реклами, аналітика), державні установи – для ідентифікації та надання послуг. Водночас такий обсяг обробки даних підвищує ризики витоку, зловживань, несанкціонованого доступу чи маніпуляцій.

У цифрову епоху персональні дані перебувають під постійною загрозою з боку як кіберзлочинців, так і недобросовісних компаній чи інституцій. Серед основних типів загроз можна виділити:

- Фішингові атаки – використання підроблених вебсайтів, електронних листів чи повідомлень для отримання доступу до логінів, паролів та іншої конфіденційної інформації.
- Соціальна інженерія – маніпулятивні методи впливу на людину, які змушують її самостійно надати свої дані.
- Використання шкідливого ПЗ – програми-віруси або шпигунське ПЗ , які здатні зчитувати дані з пристрою користувача, включаючи натискання клавіш, знімки екрана, або отримувати доступ до вебкамери чи мікрофона.
- Витоки даних із баз державних або приватних компаній – наприклад, через слабкий захист серверів, хакерські атаки або помилки персоналу.
- Недобросовісне використання даних компаніями – зокрема, передача третім особам без згоди користувача, або збирання надмірного обсягу інформації без законних підстав [2].

Такі загрози призводять не лише до втрати конфіденційності, а й до серйозних матеріальних збитків та репутаційних втрат.

Захист персональних даних є багаторівневим процесом, що включає технічні, організаційні, правові та поведінкові заходи:

Технічні методи:

- Шифрування даних під час передачі та зберігання.
- Двофакторна автентифікація (2FA) – підтвердження входу через SMS, додаток або апаратний ключ.
- Використання антивірусного ПЗ та фаєрволів.
- VPN – захист трафіку в публічних мережах.
- Регулярне оновлення програмного забезпечення – усунення вразливостей у системі.
- Організаційні заходи:
  - Визначення рівнів доступу до даних.
  - Проведення аудитів безпеки.
  - Навчання персоналу правилам обробки та захисту даних.
- Правові методи:
  - Використання договорів про конфіденційність (NDA).
  - Дотримання норм законів щодо обробки персональних даних.
- Поведінкова гігієна:
  - Не розкривати особисту інформацію в публічному доступі без потреби.
  - Обережність із підозрілими посиланнями, листами, повідомленнями.
  - Регулярна зміна паролів та використання унікальних комбінацій.

В Україні правовий захист персональних даних регулюється насамперед Законом України «Про захист персональних даних», ухваленим у 2010 році. Закон визначає:

- принципи обробки персональних даних;
- права суб'єктів персональних даних (у т.ч. право на доступ, уточнення, видалення);
- обов'язки володільців та розпорядників даних;
- повноваження уповноваженого органу з захисту даних.

Окрім того, в Україні діють норми Цивільного кодексу, Законів про інформацію, про електронні комунікації, а також Кримінального кодексу, де передбачена відповідальність за незаконне збирання та поширення конфіденційної інформації.

Важливо зазначити, що Україна поступово адаптує своє законодавство до європейських стандартів – зокрема, Регламенту ЄС 2016/679 (GDPR), що є зразком у сфері захисту персональних даних на міжнародному рівні [3].

Хоча нормативна база в Україні вже створена, практична реалізація норм поки що має низку викликів:

- низький рівень цифрової грамотності серед громадян;
- часті витоки даних з державних реєстрів та комерційних платформ;
- обмежені повноваження і ресурси уповноваженого органу з захисту даних;

- недостатня відповідальність організацій за порушення правил обробки інформації.

Водночас держава робить кроки до покращення ситуації. Наприклад, у 2021 році оновлено Стратегію кібербезпеки України, де захист персональних даних є однією з ключових складових. Активно працює CERT-UA – урядова команда реагування на комп'ютерні інциденти, яка допомагає запобігати атакам на критичну інфраструктуру та дані громадян.

Велику роль також відіграють громадські ініціативи (наприклад, StopFake, Digital Security School) та міжнародні партнери, які допомагають Україні в побудові ефективної системи кіберзахисту.

У цифрову епоху захист персональних даних є ключовим елементом кібербезпеки особи та держави. Зростання обсягів інформації та активне її використання підвищують ризики несанкціонованого доступу, витоків і зловживань [4].

Незважаючи на наявність правового регулювання в Україні, існують проблеми з практичною реалізацією – низький рівень цифрової грамотності, часті витоки даних, обмежені повноваження контролюючих органів.

Для ефективного захисту потрібен комплексний підхід: технічні засоби, правові норми, організаційні заходи та цифрова культура серед користувачів. Лише спільними зусиллями держави, бізнесу та громадян можна забезпечити безпеку персональних даних у сучасному інформаційному середовищі.

Список використаних джерел:

1. *CERT-UA*. URL: https://cert.gov.ua/.
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України; Стратегія від 26.08.2021 № 447/2021. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
3. GDPR. Complete guide to GDPR compliance. URL: https://gdpr.eu/.
4. dss380. Безпека в умовах війни. URL: https://dss380.org/useful-information/.

Ключові слова: Захист персональних даних, кібербезпека, цифрові загрози, конфіденційність, витік даних.

Keywords: Personal data protection, cybersecurity, digital threats, privacy, data leakage.