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

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

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

5. Трофименко О. Г., Соколов А. В., Чикунов П. О., Ахмаметьєва Г. В., Манаков С. Ю. Штучний інтелект у військовій кіберсфері. *Технології та інжиніринг.* 2024. № 4 (21). С. 85-92. URL: https://doi.org/10.30857/2786-5371.2024.4.8.

Ключові слова: штучний інтелект, ШІ, машинне навчання, ІТ-галузь, ІТ-кар'єра, конкурентоспроможність.
Keywords: artificial intelligence, AI, machine learning, IT industry, IT career, competitiveness.

Чанишев Рашид Ібрагімович
Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат юридичних наук, доцент

PROTECTEU – НОВА ВНУТРІШНЯ СТРАТЕГІЯ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Європейською комісією 1 квітня 2025 року було презентовано громадськості нову безпекову стратегію для країн Євросоюзу, що отримала назву «ProtectEU». Завданням цієї стратегії є посилення можливостей Європейського Союзу щодо забезпечення захисту громадян від багатоаспектних загроз сучасності шляхом створення вдосконаленої нормативно-правової бази, орієнтованої на розширення механізмів транскордонного співробітництва та забезпечення належного рівня інформаційного обміну між державами-членами ЄС, а також посилення координаційної ролі загальноєвропейських інституцій у боротьбі зі злочинністю та кіберзагрозами [1].

Нова стратегія прийшла на зміну попередній: «Стратегії Союзу безпеки ЄС 2020-2025 рр.» (Security Union Strategy), що створила основу для координації заходів із боротьби з тероризмом, організованою злочинністю та кіберзагрозами. Водночас ProtectEU доповнює презентовану 26 березня 2025 року «Стратегію Європейського Союзу із забезпечення готовності» (Preparedness Union Strategy), орієнтовану на зміцнення спроможності ЄС запобігати, виявляти й ефективно реагувати на широкий спектр криз – від природних катастроф та пандемій до кібератак і гібридних загроз, та презентований Європейською комісією 19 березня 2025 року стратегічний документ «White Paper for European Defence – Readiness 2030», що має на меті зміцнити оборонне співробітництво та промисловий потенціал країн ЄС.

За словами комісара ЄС із внутрішніх справ Магнуса Бруннера (Magnus Brunner), основною метою стратегії ProtectEU є назріла необхідність зміни менталітету і способу мислення щодо безпеки на державному рівні для всіх країн, що входять до Євросоюзу [2].

У документі наголошується, що наразі спостерігається зростання гібридних загроз як з боку низки ворожих («hostile») держав, так і з боку організованих

злочинних мереж, окремих злочинців і терористів, які активно діють в Інтернеті. Зазначається, що дії злочинців часто спонсоруються на державному рівні, у зв'язку з чим європейським країнам необхідно переглянути свій підхід до внутрішньої безпеки, оскільки ці гібридні впливи підривають демократію і громадський порядок.

У зв'язку з цим наголошується, що за даними Європолу, в переважній кількості випадків розслідування злочинів нині пов'язане з доступом до цифрової інформації, оскільки практично вся інформація зараз створюється, передається і використовується в цифровому вигляді. При цьому практично вся цифрова інформація зберігається і передається в зашифрованому вигляді, що вкрай ускладнює проведення розслідування злочинів.

З цієї причини запропоновано низку заходів, що дають змогу виправити становище, що склалося.

Зокрема, планується розширення обміну розвідувальними даними між державами-членами за допомогою SIAC (Single Intelligence Analysis Capacity) – «Єдиного центру аналітики розвідданих», що діє в рамках Європейської служби зовнішніх зв'язків (EEAS) і об'єднує військові та цивільні розвідувальні структури Європейського Союзу.

Передбачається, що у 2026 р. ЄС запропонує реорганізувати Європол і Frontex (повна назва Frontex – European Border and Coast Guard Agency) – агентство Європейського Союзу, що координує питання прикордонної та морської охорони зовнішніх кордонів ЄС. У рамках модернізації, крім усього іншого, планують збільшити штат Frontex із 10 до 30 тис. осіб.

Європол буде модернізовано більш кардинально: його перетворять на поліцейське агентство, призначене, крім усього іншого, для проведення транскордонних розслідувань із використанням найсучасніших технологій цифрової криміналістики та в тісній співпраці як із власне державами-членами ЄС, так і з іншими агенціями Європейського Союзу, як-от Eurojust (European Union Agency for Criminal Justice Cooperation), Європейською прокуратурою EPPO (European Public Prosecutor's Office) та агенцією ЄС із кібербезпеки ENISA (European Union Agency for Cybersecurity).

Для підвищення ефективності спільних операцій буде створено Європейську систему оперативного зв'язку (European Critical Communication System) – захищену платформу обміну конфіденційною інформацією, яка об'єднає екстрені служби (поліцію, швидку допомогу та ін.) різних країн [3].

Ще одним ключовим елементом стратегії є розробка «дорожньої карти щодо забезпечення можливості законного та ефективного доступу правоохоронних органів до даних», включно з комунікаціями, якими передаються зашифровані дані.

Ця ініціатива зачіпає, насамперед, постачальників месенджерів та інших платформ електронного зв'язку. Стратегія передбачає можливість створення системних вразливостей (бекдорів) у криптографічних протоколах, які вони ви-

користовують, для забезпечення доступу правоохоронних органів до конфіденційної інформації в рамках чинного законодавства.

Такий підхід, безумовно, викличе багато запитань та заперечень. Але, як обіцяє Магнус Бруннер, при цьому «будуть знайдені рішення, що гарантують право на недоторканність приватного життя».

Незважаючи на зростаючу стурбованість з боку технологічних компаній і правозахисних організацій, розробники стратегії підкреслюють, що відповідні заходи будуть спрямовані на забезпечення балансу між кібербезпекою, захистом персональних даних та ефективним розслідуванням злочинів. У документі вказується, що створюваний правовий режим має гарантувати дотримання основних прав і свобод, одночасно забезпечуючи можливість доступу до зашифрованих даних у суворо регламентованих випадках.

Як стверджується в документі, використання технології наскрізного шифрування (end-to-end encryption) організованою злочинністю призвело, зокрема, і до зростання тероризму, і до можливості передавання нелегального контенту мережею Інтернет.

Ще 21 лютого 2025 року компанія Apple оголосила про те, що відключає можливість використання користувачами, які проживають у Великій Британії, функції Advanced Data Protection (механізм захисту даних, реалізований Apple для користувачів пристроїв iOS, iPadOS і macOS, що дає змогу використовувати наскрізне шифрування (end-to-end encryption) для даних, які передають і зберігають в iCloud) [4].

Це відключення стало відповіддю на вимогу до компанії Apple з боку уряду Великої Британії надати можливість отримання повного доступу до даних користувачів, що зберігаються на хмарних серверах Apple, зокрема й до даних, захищених наскрізним шифруванням.

Цю вимогу, яка доволі серйозно порушує прийняті в сучасних демократичних країнах принципи, негативно оцінили експерти з питань конфіденційності та безпеки, які стверджували, що виконання цієї вимоги створить прецедент для авторитарних країн.

У відповідь на фактичне прохання щодо впровадження бекдора в програмне забезпечення представники Apple заявили: «Як ми вже багато разів говорили, ми ніколи не створювали бекдор або майстер-ключ для будь-якого з наших продуктів або послуг і ніколи не будемо» [5].

На цьому фоні стратегія ProtectEU почала викликати побоювання, пов'язані з тим, що її успішна реалізація може призвести до посилення нагляду за громадянами та потенційного порушення прав на конфіденційність, надання можливості доступу правоохоронним органам до зашифрованих даних та до особистої інформації користувачів, порушення прав та свобод, включно з правом на анонімність і свободу вираження поглядів в Інтернеті. При цьому наголошується, що розроблення стратегії відбувалося без участі громадянського суспільства та експертів у сфері прав людини і без широкого громадського обговорення, що

викликає певні сумніви щодо легітимності пропонованих заходів і їхньої відповідності демократичним принципам.

Стратегія ProtectEU є досить амбітним планом зі зміцнення внутрішньої безпеки ЄС, однак існують серйозні побоювання щодо того, що її практична реалізація призведе до порушення прав і свобод громадян. Для досягнення балансу між безпекою і захистом прав людини необхідно створити міждержавну громадську організацію, завданням якої буде контроль за практичною реалізацією пропонованих у стратегії заходів для запобігання зловживанням з боку правоохоронних і розвідувальних структур.

Список використаних джерел:

1. Commission unveils ProtectEU – a new European Internal Security Strategy. URL: https://surl.li/zsucgf (Last access: 10.04.2025).

2. Verbatim report of proceedings Tuesday, 1 April 2025 – Strasbourg. URL: https://surl.li/rhhoce (Last access: 10.04.2025).

3. Commission presents ProtectEU Internal Security Strategy. URL: https://surl.li/rbyrda (Last access: 11.04.2025).

4. Apple pulls iCloud end-to-end encryption feature for UK users after government demanded backdoor. URL: https://surl.li/uekqby (Last access: 11.04.2025).

5. We believe security shouldn't come at the expense of individual privacy. URL: https://www.apple.com/privacy/government-information-requests (Last access: 11.04.2025).

Ключові слова: Євросоюз, внутрішня безпека ЄС, стратегія безпеки, транскордонні операції, криптографічний захист, цифрові свободи.

Keywords: EU, EU internal security, security strategy, cross-border operations cryptographic defence, digital freedoms.

Чикунов Павло Олександрович
Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент

ПРОЄКТУВАННЯ ВЕБОРІЄНТОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ УНІВЕРСАЛЬНОЇ ПЛАТФОРМИ WINDOWS

Метою роботи є комплексне дослідження, що спрямоване на підтримку процесу проєктування веборієнтованих інформаційних систем (ВІС) для продажу товарів через інтернет із використанням технологій, що забезпечують високу продуктивність, зручність використання та безпеку даних. Розробка таких систем набуває актуальності в умовах стрімкого розвитку цифрових технологій і зростання попиту на онлайн-послуги, що дозволяє підпри-