МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

ISSN 3083-6557 print

НАУКОВІ ПРАЦІ МАУП

Проблеми модернізації України

Випуск 1 (48), 2025

Київ
2025

УДК 330-339; 321.7; 159.9
М58

Схвалено Вченою радою Міжрегіональної Академії управління персоналом (протокол № 4 від 28.05.2025)

Редакційна колегія:
С. В. Храпатий (голова), д-р фіз.-мат. наук, проф.
І. А. Семенець-Орлова, д-р наук з держ. упр., проф.
Я. М. Раєвська, д-р психол. наук, проф.
С. О. Лисенко, д-р юрид. наук, проф.
А. І. Федосов, д-р мед. наук, проф.
М. І. Зубрицький, д-р. юрид. наук
О. М. Гордієнко, канд. техн. наук
В. І. Меджебель (*Чуєнко*), канд. юрид. наук
Л. М. Крива, канд. істор. наук
І. М. Капеліста (виконавчий редактор), канд. наук з держ. упр.
Є. Я. Черняк

Матеріали подано в авторській редакції.
Відповідальність за зміст та орфографію матеріалів несуть автори.

Міжрегіональна Академія управління персоналом.
М58 Наукові праці МАУП. Проблеми модернізації України / редкол.: С. В. Храпатий (голова) [та ін.]. Вип. 1 (48). Київ: Міжрегіональна Академія управління персоналом, 2025. 686 с. Бібліогр. в кінці ст.

У збірнику висвітлено матеріали X Міжнародної науково-практичної конференції "Розбудова інноваційних економіки, менеджменту та освіти в умовах нової соціальної реальності" (Київ, Міжрегіональна Академія управління персоналом, 20–22 травня 2025 р.).

Наведено тези доповідей учасників науково-практичної конференції МАУП з проблематики широкого кола аспектів процесу системної модернізації України.

Для науковців, громадсько-політичних діячів, студентів, а також усіх, хто цікавиться розвитком Української держави і світовим досвідом проведення модернізаційних процесів.

Видається з 2001 року.
Періодичність: 1 раз на квартал.
Засновник: *ПрАТ "ВНЗ "Міжрегіональна Академія управління персоналом".*
УДК 330-339; 321.7; 159.9

© Міжрегіональна Академія управління персоналом (МАУП), 2025

А. П. Гринчук
Проведення оцінювання діяльності громадських організацій та установ, як окремий вид оціночної діяльності *506*

Ю. Е. Пашко
Охорона земель в містах а також інших населених пунктах *508*

Д. В. Святецький
Банкрутство фермерських господарств у новій реальності: виклики економіки та менеджменту *510*

Р. О. Поливач
Економічні санкції як відповідь міжнародного співтовариства на ядерну програму Ірану *513*

Я. В. Кушнір
Оренда території Гуантанамо як виклик принципу територіальної цілісності держав у міжнародному публічному праві *515*

А. А. Тернавська
Деякі аспекти криміналізації суспільно небезпечних діянь у сфері радіоекологічної безпеки *518*

СУЧАСНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

С. О. Лисенко
Формування державної політики у сфері інформаційної безпеки: пріоритети та інституційне забезпечення *521*

І. В. Сервецький
Моральна риторика, як ширма під час війни: між словом і смертю *523*

С. Г. Голубицький
Фінансові ризики в умовах сучасної геополітичної ситуації, як загроза економічній безпеці *525*

А. І. Тараненко
Забезпечення інформаційної безпеки фінансових установ в системі державного управління: сучасна методологія *528*

О. І. Ткаченко
Ідентифікація джерел інформації щодо викликів і загроз безпеці, крізь призму публічного управління *530*

О. В. Поляков
Перспективи розвитку нотаріату в умовах цифровізації: правовий аспект *532*

О. І. Полотнянко
Технічні інформаційні загрози виборчому процесу: правовий аспект *535*

Д. В. Шейбут
Сучасні міграційні процеси в ЄС: безпековий вимір *537*

О. І. ПОЛОТНЯНКО
канд. екон. наук, докторант,
доцент кафедри адміністративного, фінансового та банківського права
Навчально-наукового інституту права імені князя Володимира Великого, МАУП
e-mail: ksenijapolo21@gmail.com
https://orcid.org/0009-0008-7319-421X

ТЕХНІЧНІ ІНФОРМАЦІЙНІ ЗАГРОЗИ ВИБОРЧОМУ ПРОЦЕСУ: ПРАВОВИЙ АСПЕКТ

У сучасному цифровому середовищі виборчий процес дедалі більше залежить від інформаційно-комунікаційних технологій, що водночас розширює можливості демократичного волевиявлення громадян, але й створює нові вектори уразливості з погляду інформаційної безпеки. Технічні інформаційні загрози, що постають перед виборчим процесом, мають складну, мультифакторну природу, охоплюючи як кібератаки на інфраструктуру, так і втручання у бази даних виборців, маніпуляції алгоритмами підрахунку голосів, блокування інформаційних ресурсів, або впровадження шкідливого програмного забезпечення у системи електронного голосування [1]. Дана ситуація зумовлює необхідність переосмислення правового забезпечення виборчого процесу через призму сучасних загроз, що пов'язані з використанням технологій для впливу на елементи виборчої інфраструктури.

Аналіз технічних інформаційних загроз у виборчому процесі передбачає виділення трьох основних рівнів: 1) загрози на рівні критичної інфраструктури (сервери, канали зв'язку, центри зберігання даних); 2) загрози на рівні програмного забезпечення (електронні реєстри, автоматизовані системи обробки результатів голосування); 3) загрози на рівні кінцевого користувача (інтерфейси для онлайн-голосування, електронні скриньки, SMS-підтвердження тощо). Кожен із цих рівнів може бути об'єктом кібератак або інфільтрації із боку як внутрішніх, так і зовнішніх суб'єктів, включно з хакерськими угрупованнями, що діють в інтересах іноземних держав. При цьому особливу загрозу становлять цілеспрямовані (APT) атаки, які зазвичай є частиною ширших інформаційно-психологічних кампаній зі зриву або делегітимізації виборів.

Правовий аспект реагування на зазначені загрози є недостатньо сформованим, що пов'язано з відставанням національного законодавства від темпів цифровізації виборчих технологій. Чинна нормативно-правова база України містить окремі положення щодо кібербезпеки, захисту персональних даних, безпеки критичної інфраструктури та виборчого законодавства, проте вони не утворюють єдиного узгодженого комплексу, здатного ефективно протидіяти технічним загрозам у контексті виборчого процесу. Наприклад, Закон України "Про основні засади забезпечення кібербезпеки України" визначає загальні принципи захисту кіберпростору, однак не деталізує механізмів превенції атак на виборчі сервери чи електронні реєстри [2]. Аналогічно, норми Виборчого кодексу України здебільшого зосереджені на процедурних аспектах голосування та підрахунку, майже не зачіпаючи ризиків, пов'язаних із використанням інформаційних технологій.

Проблемною є також відсутність належної імплементації міжнародних стандартів у сфері кіберзахисту виборчих процесів. У таких країнах, як Естонія, США, Франція,

Нідерланди, виборча інфраструктура підпадає під спеціальний статус захищеного об'єкта критичної інфраструктури, із закріпленням окремих протоколів резервного зберігання даних, багаторівневого автентифікаційного контролю, незалежного аудиту ПЗ, а також обов'язкової участі спеціалізованих агенцій кіберзахисту у процесі виборчого адміністрування [3]. В Україні ж питання захисту інформаційно-аналітичної системи "Вибори" досі вирішуються в контексті загальних ІТ-закупівель ЦВК та не підпадають під незалежний контроль у сфері кібербезпеки.

Особливої уваги потребує проблема правового регулювання електронного голосування, яке теоретично може забезпечити зручність і доступність виборчого процесу для громадян за кордоном, військовослужбовців або осіб з обмеженою мобільністю. Однак будь-яка система дистанційного волевиявлення автоматично включає високі ризики інформаційного впливу: перехоплення сеансів, заміна даних, підміна результатів або шкідливе оновлення системного ПЗ. У більшості розвинених країн, де такі моделі впроваджуються, законодавство передбачає сувору процедуру сертифікації програмного забезпечення, багаторівневе шифрування, блокчейн-технології для забезпечення прозорості транзакцій, а також зовнішній технічний аудит з боку незалежних організацій. В Україні ж будь-яка спроба запровадження е-голосування вимагає створення нового законодавчого механізму — з чітким визначенням відповідальних органів, стандартів захисту, механізмів перевірки достовірності результатів та відповідальності за технічні збої чи втручання.

У зв'язку з вищезазначеним необхідною є розробка спеціального розділу у Виборчому кодексі України, присвяченого інформаційно-технічній безпеці виборчого процесу. Такий розділ має містити: визначення термінів (інформаційна атака, інцидент безпеки, технічний аудит тощо), структуру повноважень між ЦВК, Держспецзв'язку, СБУ, Національним агентством з кібербезпеки (після його створення), порядок сертифікації ПЗ, стандарти зберігання даних, процедури реагування на інциденти, а також положення про кримінальну та адміністративну відповідальність за втручання в технічні компоненти виборчого процесу. Важливо, щоб такий розділ передбачав обов'язкове залучення зовнішніх аудиторів — як національних, так і міжнародних, для забезпечення незалежної перевірки коду, системних журналів та процедур резервування даних.

З огляду на стрімку еволюцію технічних загроз і засобів впливу, необхідною є постійна адаптація національного законодавства до сучасних викликів, а також гармонізація з нормами Європейського Союзу. Зокрема, Рекомендації Ради Європи щодо електронної демократії (CM/Rec(2009)1) [4], Загальні принципи захисту критичної інформаційної інфраструктури (CIIP), а також Директива NIS 2 (Directive (EU) 2022/2555) мають бути імплементовані до українського нормативного поля. Варто також брати до уваги досвід таких ініціатив, як TIBER-EU (Threat Intelligence Based Ethical Red-teaming) — програми з моделювання кіберзагроз у фінансовому секторі, які можуть бути адаптовані і до виборчої сфери. У даному контексті важливим є створення національної методики тестування виборчих систем на стійкість до технічних атак — із законодавчим закріпленням вимог до тестів, відповідальних структур, порядку аналізу результатів.

Джерела

1. *Редчиць О. С.* Моніторинг загроз виборчим процесам: сучасний стан в Україні та міжнародний досвід впровадження. *Вчені записки ТНУ імені В. І. Вернадського*. Серія: Публічне управління та адміністрування. 2022. Т. 33 (72), № 2. С. 86–93. DOI: https://doi.org/10.32838/TNU-2663-6468/2022.2/15

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради* (ВВР). 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. *Гриськов М. М.* (2025). Правове регулювання здійснення електронного голосування за правом Європейського Союзу в контексті проблематики впровадження електронного голосування в Україні. *Проблеми сучасних трансформацій.* Серія: право, публічне управління та адміністрування, (16). URL: https://doi.org/10.54929/2786-5746-2025-16-02-06
4. Recommendation CM/Rec(2009)1 of the Committee of Ministers to member states on electronic democracy (e-democracy) : adopted by the Committee of Ministers on 18 February 2009 at the 1049th meeting of the Ministers' Deputies. Strasbourg : Council of Europe Publishing, 2009. 47 p. (Legal instruments). URL: https://www.coe.int/t/dgap/goodgovernance/activities/key-texts/recommendations/recommendation_cm_rec2009_1_en_pdf.pdf

Д. В. ШЕЙБУТ

канд. юрид. наук, доцент кафедри національної безпеки
Інституту безпеки ПрАТ "ВНЗ "Міжрегіональна Академія управління персоналом"

СУЧАСНІ МІГРАЦІЙНІ ПРОЦЕСИ В ЄС: БЕЗПЕКОВИЙ ВИМІР

Міграційні процеси в Європейському Союзі у XXI столітті стали однією з найгостріших соціально-політичних проблем, що вимагають комплексного аналізу з позицій безпеки. Масовий наплив мігрантів, зумовлений як економічними труднощами, так і воєнними конфліктами, особливо на Близькому Сході, в Африці та Азії, став викликом не лише для національних політик окремих держав, а й для загальноєвропейського простору безпеки. У зв'язку з цим актуалізується концепт "міграційної безпеки", який в науковому дискурсі дедалі частіше трактується як складова національної та регіональної безпеки, що охоплює політичні, соціальні, економічні та культурні виміри. Сутність безпекового виміру міграції полягає у потенційній загрозі, яку становлять як неконтрольовані потоки мігрантів, так і неспроможність інституцій ЄС до своєчасного реагування на новітні виклики глобального характеру.

Особливої уваги вимагає аналіз структурних чинників, що сприяють нестабільності всередині ЄС у контексті міграції. До них можна віднести фрагментарність імміграційної політики, відсутність єдиного центру прийняття рішень щодо розподілу біженців, а також зростання популізму і праворадикальних настроїв у країнах-членах. Посилення контролю на зовнішніх кордонах ЄС, ініціативи з реформування Шенгенської зони, створення спільних агентств з охорони кордонів, таких як Frontex, свідчать про прагнення Брюсселя інституціоналізувати захист безпеки через обмеження мобільності осіб, що не мають легального статусу перебування. Проте ці кроки не завжди супроводжуються ефективною інтеграційною політикою, що породжує сегрегацію, соціальне відчуження і зростання конфліктності в приймаючих державах. Таким чином, безпековий вимір сучасної міграції в ЄС не може бути зведений лише до фізичного контролю за кордонами, оскільки безпека охоплює також і соціальну злагоду, стабільність інституцій та рівень довіри між різними етнічними й культурними групами.