НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет цивільної та господарської юстиції
Кафедра приватного права
Кафедра права інтелектуальної власності та патентної юстиції

ІТ-ПРАВО, КІБЕРБЕЗПЕКА ТА ШІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

МАТЕРІАЛИ
Всеукраїнської наукової конференції

28 березня 2026 р.

Одеса
Фенікс
2026

УДК 342.95:343.32 (477):351.863
І-92

За загальною редакцією
доктора юридичних наук, професора **Є. О. Харитонова**,
докторки юридичних наук, професорки **І. В. Давидової**

Упорядники-укладачі:

Давидова І. В. – доктор юридичних наук, професор, професор кафедри приватного права Національного університету «Одеська юридична академія»;

Калітенко О. М. – кандидат юридичних наук, доцент, професор кафедри приватного права Національного університету «Одеська юридична академія»;

Бобейко Н. І. – лаборантка кафедри приватного права Національного університету «Одеська юридична академія».

І-92 **ІТ-право, кібербезпека та ШІ в умовах гібридної війни** : мате-ріали Всеукр. наук. конф. (Одеса, 28 берез. 2026 р.) / за заг. ред.: д-ра юрид. наук, проф. Є. О. Харитонова, д-ра юрид наук, проф. І. В. Давидової. Одеса : Фенікс, 2026. 300 с. DOI: https://doi.org/10.32837/11300.33701

ISBN 978-617-8763-22-0

Збірник містить матеріали доповідей, присвячені актуальним проблемам ІТ-права, кібербезпеки, цифрової трансформації суспільних відносин, правового регулювання штучного інтелекту та захисту інформації в умовах гібридної війни, які були оприлюднені на Всеукраїнській науковій конференції 26 березня 2026 року в Національному університеті «Одеська юридична академія».

Збірник спрямований на ознайомлення науковців, викладачів, здобувачів освіти, практикуючих юристів, фахівців у сфері інформаційних технологій і кібербезпеки з результатами сучасних досліджень щодо правових, організаційних і технологічних аспектів функціонування цифрового середовища в умовах сучасних викликів. Матеріали видання можуть бути використані в науковій, освітній і практичній діяльності, а також під час подальшого вдосконалення правового регулювання цифрових відносин і забезпечення кібербезпеки України.

342.95 : 343.32 (477) : 351.863

Матеріали видано за авторською редакцією.
Повну відповідальність за достовірність і якість поданого матеріалу несуть учасники Всеукраїнської наукової конференції, їхні наукові керівники, рецензенти і структурні підрозділи вищих навчальних закладів та установ, які рекомендували ці матеріали до друку.

ISBN 978-617-8763-22-0

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ
Всеукраїнської наукової конференції

Харитонов Є. О. – завідувач кафедри приватного права Національного університету «Одеська юридична академія», д-р юрид. наук, проф. (голова);

Федотов О. П. – начальник науково- дослідної частини, професор кафедри морського, митного та інформаційного права, д-р юрид. наук, проф. (заступник голови);

Харитонова О. І. – завідувачка кафедри права інтелектуальної власності і патентної юстиції, д-р юрид. наук, проф.;

Галупова Л. І. – доцентка кафедри права інтелектуальної власності і патентної юстиції, канд. юрид. наук, доц.;

Зубар В. М. – професор кафедри приватного права, канд. юрид. наук, проф.;

Калітенко О. М. – професорка кафедри приватного права, канд. юрид. наук, доц.;

Кривенко Ю. В. – доцентка кафедри приватного права, канд.юрид. наук, доц.;

Токарева В. О. – доцентка кафедри приватного права, д-р юрид. наук,доц.;

Бобейко Н. І. – лаборантка кафедри приватного права.

. ,

Рябченко Вікторія Олександрівна
аспірантка 3-го року навчання кафедри приватного права
Національного університету «Одеська юридична академія»

ВИКОРИСТАННЯ ОНЛАЙН ІГОР ТА МЕСЕНДЖЕРІВ ЯК ІНСТРУМЕНТУ ВЕРБУВАННЯ: ВИКЛИКИ ДЛЯ ІТ-ПРАВА

В умовах війни, коли соціальні та економічні структури дестабілізовані, кіберпростір остаточно став ще одним фронтом гібридної війни. Поряд із масовими кампаніями дезінформації та маніпуляціями зі сторони країни-агресора все частіше фіксуються випадки онлайн-вербування українських громадян за допомогою ігрових платформ, соціальних мереж та різних месенджерів з метою виконання розвідувальних, диверсійних чи пропагандистських завдань.

Вербувальники зазвичай діють за чітко відпрацьованою схемою. За останніми даними, представники російських спецслужб продовжують свою діяльність, вдаючись до дедалі більш цинічних і протиправних методів. Активно використовують месенджери та соціальні мережі, надсилаючи громадянам підроблені повістки, залякуючи неіснуючими справами [2]. У деяких випадках вони пропонують фіктивну допомогу у врегулюванні вигаданих проблем в обмін на виконання певних розвідувальних або підривних завдань стосовно військових об'єктів або об'єктів критичної інфраструктури. Російські спецслужби використовують сайти й сервіси онлайн-знайомств для вербування українців. Вони створюють фейкові жіночі акаунти, налагоджують спілкування з чоловіками та виманюють особисті дані. Після цього з жертвою зв'язується так званий «співробітник СБУ», який звинувачує її у контактах із представницею ворожих спецслужб. Під приводом уникнення відповідальності, шляхом шантажу, особі пропонують співпрацювати, змушуючи виконувати розвідувальні чи диверсійні завдання. Спецслужби країни-агресора використовують бот-мережі в соціальних мережах і месенджерах для вербування українців. Такі боти імітують живе спілкування, створюють довірливу атмосфе-

ру та поступово залучають користувача до спільних завдань чи закритих груп. Через них збирають персональні дані, відстежують емоційний стан людини та відбирають найбільш вразливих осіб для подальшої індивідуальної роботи з кураторами. Вербувальники також створюють оголошення про нібито високооплачувану роботу – часто з формулюваннями на кшталт «підробіток онлайн», «робота, можна без досвіду», «година часу і гроші твої». Такі повідомлення розміщуються у соціальних мережах, ігрових чатах, телеграм-каналах чи на платформах з пошуку роботи.

Організатори вербувальних схем постійно знаходять нові можливості для обходу державних обмежень, адаптуючи свої методи до розвитку цифрових технологій.

Одним із очевидних результатів цифровізації є створення криптовалюти. Біткоїн та інші криптовалюти змінили не тільки фінансову систему, а й способи та засоби протиправної діяльності. Цифрова інфраструктура створила сприятливе середовище для фінансування терористичних організацій [3, с. 72]. В реаліях сьогодення викликом стає використання внутрішньо-ігрових систем та цифрових активів, таких як віртуальні монети, токени, скіни чи предмети обміну, як інструменту для проведення нелегальних фінансових операцій, пов'язаних із вербуванням. Фіксується тенденція, коли організатори уникають традиційних фінансових каналів, переходячи до розрахунків усередині ігрових платформ або з використанням криптовалют. Такі транзакції значно ускладнюють відстеження руху коштів і створюють правові прогалини і у результаті віртуальні предмети стають «сірою зоною» фінансових взаєморозрахунків, де можливо здійснювати виплати за збір інформації, пропагандистську діяльність або виконання завдань розвідувального характеру.

Також проблемою залишається визначення меж відповідальності цифрових платформ за використання їхньої інфраструктури для сприяння злочинним діям. Хоча європейський законодавчий досвід, зокрема Digital Services Act (DSA), встановлює обов'язок провайдерів модерувати заборонений контент, цей механізм де-

монструє обмежену ефективність у зашифрованих месенджерах та ігрових чатах через пріоритетність таємниці приватного спілкування. У цьому контексті особливої ваги набуває Постанова Кабінету Міністрів України № 1533 від 26.11.2025 р. Вона пропонує змістити акцент із пасивного очікування скарг на активну координацію між державними органами та ІТ-сектором [1]. Відповідно до Постанови, дії, пов'язані з онлайн-вербуванням можуть бути кваліфіковані як соціально орієнтовані кіберінциденти, що дозволяє застосовувати технічні протоколи реагування, не порушуючи при цьому приватно-правову природу листування. Натомість, наприклад, діяти на рівні оперативного виявлення нетипової активності у поведінці автоматизованих систем (ботів), які використовуються для масових розсилок та пошуку потенційних жертв вербування.

Підсумовуючи, необхідно зазначити, що онлайн-вербування через ігрові платформи, сайти, месенджери демонструє прогалини правових інструментів для протидії гібридним загрозам у цифрову епоху. Використання нетрадиційних фінансових каналів, як ігрова валюта, токени чи криптовалюта, створює приховане середовище для розрахунків, що потребує адаптації норм ІТ-права. Крім того, важливим є законодавче визначення меж відповідальності цифрових платформ за безпеку їх систем та впровадження правових механізмів моніторингу обігу віртуальних грошових активів.

ЛІТЕРАТУРА:

1. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози: Постанова Кабінету Міністрів України від 26.11.2025 р. № 1533. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text

2. Російські спецслужби активізували вербування українців, видаючи себе за СБУ. *Армія FM*. URL: https://www.armyfm.com.ua/rosiiski-spetssluzhby-aktyvizuvaly-verbuvannia-ukraintsiv-vydaiuchy-sebe-za-sbu/

3. Dyntu, V., & Dykyj, O. (2021). Cryptocurrency as an instrument of terrorist financing. *Baltic Journal of Economic Studies*, 7(5), 67-72. https://doi.org/10.30525/2256-0742/2021-7-5-67-72