**Кібербезпека**

**(інформаційні злочини, інформаційний тероризм):**

***анотований бібліографічний список***

***2025. – Вип. 5 (травень). – 18 с.***

<http://www.nplu.org/article.php?id=423>

1. **Андрусяк А. До 400 млн доларів збитків: одну з найбільших криптобірж США зламали хакери** [Електронний ресурс] / Анастасія Андрусяк // Focus.ua : [вебсайт]. – 2025. – 16 трав. – Електрон. дані. *Йдеться про те, що кіберзлочинці викрали дані клієнтів американської криптовалютної біржі «Coinbase», після чого зажадали у компанії 20 млн доларів за збереження хакерської атаки в таємниці. Компанія заявила, що для заволодіння особистою інформацією клієнтів хакери «підкупили та завербували» агентів підтримки, які працюють за межами США. Зазначено, що криптобіржа виплатить винагороду в розмірі 20 млн доларів за інформацію, яка допоможе заарештувати кіберзлочинців. Компанія також пообіцяла відшкодувати збитки клієнтам, яких обманом змусили відправити кошти зловмисникам. Сума компенсації може становити від 180 до 400 млн доларів.* Текст: <https://focus.ua/uk/digital/706467-do-400-mln-dolariv-zbitkiv-odnu-z-naybilshih-kriptobirzh-ssha-zlamali-hakeri>
2. **Андрусяк А. Комп'ютери під загрозою через хакерів, які «подорожують у часі»: як захиститися** [Електронний ресурс] / Анастасiя Андрусяк // Focus.ua : [вебсайт]. – 2025. – 1 трав. – Електрон. дані. *Деталі нової тактики хакерів розкрив журналіст і експерт із технологій Курт Кнутссон, посилаючись на дані Федерального бюро розслідувань (ФБР). За його словами, ця тактика дає змогу кіберзлочинцям обійти традиційні засоби захисту. Як пояснив експерт, зловмисники використовують прострочені сертифікати безпеки, змінюючи системну дату на пристрої на час, коли ці сертифікати були ще дійсні. Таким чином, шкідливі програми, створені за допомогою цих застарілих сертифікатів, будуть визнані системою легітимними, що дасть змогу здійснити «подорож у минуле» з точки зору безпеки. Розглянуто рекомендації ФБР щодо захисту від шкідливого програмного забезпечення «Medusa»*. Текст: <https://focus.ua/uk/digital/704393-komp-yuteri-pid-zagrozoyu-cherez-hakeriv-yaki-podorozhuyut-u-chasi-yak-zahistitisya>
3. **Андрусяк А. ШІ тепер може «читати» вашу пошту Gmail та особисті документи: чому це важливо** [Електронний ресурс] / Анастасiя Андрусяк // Focus.ua : [вебсайт]. – 2025. – 21 трав. – Електрон. дані. *Йдеться про те, що модель штучного інтелекту (ШІ) Gemini від Google отримала велике оновлення, в межах якого може підключатися до Gmail, Google Docs, Drive, Calendar і багатьох інших додатків. Тепер Gemini перетворився з чат-бота з ШІ на справжнього особистого асистента. Оновлення обіцяє більш «розумну» допомогу, однак має ризики з точки зору конфіденційності. У Google стверджують, що Gemini не буде використовувати дані з особистих документів і пошти для навчання своїх публічних ШІ-моделей, при цьому в експертів залишаються деякі побоювання, пов'язані з безпекою. Розглянуто, як обмежити можливості Gemini.* Текст: <https://focus.ua/uk/digital/707139-shi-teper-mozhe-chitati-vashu-poshtu-gmail-ta-osobisti-dokumenti-chomu-ce-vazhlivo>
4. **Батраченко Т. С. Захист державної таємниці в умовах гібридної війни досвід України та інших країн** [Електронний ресурс] / Тетяна Сергіївна Батраченко, Олександр Григорович Розгон, Інна Веніамінівна Єфімова // Наук. перспективи. – 2025. – № 3. — С. 948-961. *Здійснено комплексне дослідження проблеми захисту державної таємниці в умовах гібридної війни з урахуванням новітніх викликів і загроз у сфері національної безпеки. Зазначено, що у контексті збройної агресії РФ проти України особливої актуальності набуває питання забезпечення належного правового та технічного режиму охорони інформації з обмеженим доступом. Вказано, що гібридна війна, в основі якої лежить поєднання військових, інформаційних, кібератак і психологічних операцій, істотно підвищує вразливість державної інформаційної системи, зокрема в частині, що стосується збереження державної таємниці. Систематизовано основні напрямки правового регулювання у цій сфері та розглянуто чинне законодавство України – закони України «Про державну таємницю», «Про основні засади забезпечення кібербезпеки України» та «Про критичну інфраструктуру». Наведено порівняльний аналіз підходів до захисту секретної інформації в Україні, Європейському Союзі (ЄС) та США. Сформульовано низку практичних рекомендацій, серед яких: створення єдиного реєстру об’єктів, що оперують державною таємницею; посилення відповідальності за порушення режиму секретності; впровадження гнучкого правового механізму реагування на нові загрози; формування національної освітньо-сертифікаційної системи підготовки фахівців у сфері інформаційної безпеки.*Текст: <http://perspectives.pp.ua/index.php/np/article/view/21935/21905>
5. **Бережна Д. NIS2 та кібербезпека: як нові правила ЄС впливають на український бізнес вже сьогодні** [Електронний ресурс] / Дар'я Бережна // Focus.ua : [вебсайт]. – 2025. – 28 трав. – Електрон. дані. *Зазначено, що у 2024 р. Європейський Союз (ЄС) затвердив нову директиву NIS2, яка стала обов’язковою для бізнесу в критичних і важливих секторах ЄС. Хоча Україна ще не є членом ЄС, вітчизняний бізнес уже відчуває вплив нових правил. Вказано, що партнери з ЄС вимагають підтвердження відповідності, а компанії змушені адаптувати підходи до кіберзахисту. Компанія «IT Specialist», яка супроводжує український бізнес у питаннях кіберстійкості, пропонує подивитися на те, як саме NIS2 змінює український ринок: від зростання атак до нових підходів щодо захисту*. Текст: <https://focus.ua/uk/ukraine/707461-nis2-ta-kiberbezpeka-yak-novi-pravila-yes-vplivayut-na-ukrajinskiy-biznes-vzhe-sogodni>
6. **Буняк В. Велика Британія повідомила про викриття російської кіберкампанії проти іноземної підтримки Україні** [Електронний ресурс] / Валерія Буняк // Детектор медіа : [інтернет-вид.]. – 2025. – 22 трав. – Електрон. дані. *Зазначено, що Велика Британія спільно з 10 країнами-союзниками викрила кіберкампанію російської розвідки проти західних логістичних і технологічних компаній, зокрема тих, що займаються наданням іноземної допомоги Україні. Про це повідомили на сайті Британського національного центру кібербезпеки (NCSC), який входить до складу Королівського військово-цивільного комітету (GCHQ). Із 2022 р. росіяни проводили зловмисну кіберкампанію проти організацій, задіяних у координації, транспортуванні та доставці підтримки Україні, а також проти компаній у секторах оборони, ІТ-послуг, морського судноплавства, аеропортів, портів і систем управління повітряним рухом у багатьох країнах-членах НАТО. Керівників організацій, які можуть опинитися під загрозою, закликали вжити негайних заходів для захисту, які включають посилення моніторингу, використання багатофакторної автентифікації з ключами доступу і забезпеченням оперативного застосування оновлень безпеки. Попередження NCSC підписали США, Німеччина, Чехія, Польща, Австралія, Канада, Данія, Естонія, Франція та Нідерланди.* Текст: [https://ms.detector.media/kiberbezpeka/post/37973/2025-05-22-velyka-brytaniya-povidomyla-pro-vykryttya-rosiyskoi-kiberkampanii-proty-inozemnoi-pidtrymky-ukraini](https://ms.detector.media/kiberbezpeka/post/37973/2025-05-22-velyka-brytaniya-povidomyla-pro-vykryttya-rosiyskoi-kiberkampanii-proty-inozemnoi-pidtrymky-ukraini/)
7. **Бурдейна О. Google виявила новий вірус РФ, який зламує політиків та активістів: як ним заражаються** [Електронний ресурс] / Олена Бурдейна // Focus.ua : [вебсайт]. – 2025. – 11 трав. – Електрон. дані. *Йдеться про те, що фахівці з кібербезпеки компанії «Google» виявили новий вірус LOSTKEYS, який походить з РФ. Зафіксовано мінімум три випадки застосування шкідливого коду, який викрадає контакти та файли політиків і громадських активістів. Вказано, що росіяни використовують підроблену «капчу» та імітують програму OSINT-аналітиків. Розглянуто, як захиститись від вірусу.* Текст: <https://focus.ua/uk/digital/705668-google-viyavila-noviy-virus-rf-yakiy-zlamuye-politikiv-ta-aktivistiv-yak-nim-zarazhayutsya>
8. **Гарькавий І. Б. Проблеми розвитку цифрової компетентності державних службовців в контексті повномасштабної війни в Україні** [Електронний ресурс] / І. Б. Гарькавий, М. Ю. Федюнін // Право та держ. упр.: зб. наук. пр. – 2024. – Вип. 4. – С. 149-153. *Досліджено виклики та особливості розвитку цифрової компетентності державних службовців в умовах повномасштабної війни в Україні. Визначено, що формування цифрових навичок залишається проблемою, особливо з урахуванням викликів інформаційної війни та кіберзагроз. Описано Рамку цифрових компетентностей для держслужбовців, що включає ІТ-грамотність, роботу з цифровим контентом, комунікацію, безпеку інформації та реалізацію політики цифровізації. Акцент зроблено на необхідності доповнення Рамки механізмами безпеки та розробленні оновленого проєкту цифрової компетентності з урахуванням сучасних викликів.* Текст: <http://www.pdu-journal.kpu.zp.ua/archive/4_2024/22.pdf>
9. **Добров В. Україна тісно співпрацює з Євроюстом для збору доказової бази та ідентифікації воєнних злочинців рф, – Олег Татаров** [Електронний ресурс] / Володимир Добров // Fakty.ua : [вебсайт]. – 2025. –
9 трав. – Електрон. дані. *Йдеться про те, що розслідування воєнних злочинів, скоєних РФ під час війни в Україні, має на меті притягнення винних до відповідальності та встановлення повної справедливості. Покаранню воєнних злочинців сприятиме спецтрибунал, над створенням якого Україна працює разом із партнерами. Про це заявив заступник керівника Офісу Президента України (ОПУ) Олег Татаров на зустрічі із президентом Агентства Європейського Союзу (ЄС) з питань співробітництва у сфері кримінального правосуддя (Євроюст) Міхаелем Шмідом. За його словами, українські правоохоронці та Офіс Генерального прокурора тісно співпрацюють з Євроюстом, обмінюючись інформацією під час формування доказової бази та встановлення осіб, які вчиняли воєнні злочини на території України. Крім того, учасники зустрічі обговорили напрями вдосконалення наявних механізмів притягнення до відповідальності осіб за скоєння економічних, корупційних та інших злочинів на території України. М. Шмід зазначив, що Євроюст готовий обговорювати подальшу взаємодію з українськими правоохоронцями щодо боротьби з міжнародними злочинцями, зокрема кіберзлочинцями.* Текст: <https://fakty.ua/454098-ukraina-tesno-sotrudnichaet-s-evroyustom-dlya-sbora-dokazatelnoj-bazy-i-identifikacii-voennyh-prestupnikov-rf-oleg-tatarov>
10. **Дронова А. Цифрова безпека вимагає співпраці на всіх рівнях: підсумки InfoSec Ukraine 2025 у Києві** [Електронний ресурс] / Аліна Дронова // Fakty.ua : [вебсайт]. – 2025. – 8 трав. – Електрон. дані. *Зазначено, що 06.05.2025 у Києві пройшла конференція «InfoSec Ukraine 2025» – одна з ключових подій у сфері інформаційної безпеки та кібербезпеки, яка цього року зібрала понад 800 учасників із різних країн. Захід став точкою перетину стратегічних рішень, міжнародного досвіду та локального бачення того, як Україна може посилити свою цифрову оборону в умовах гібридної війни та постійних атак на критичну інфраструктуру. Конференція об’єднала представників уряду, технологічного бізнесу, міжнародних організацій та провідних аналітичних центрів. Вони обговорювали, як змінюється ландшафт інформаційної безпеки, що означає цифрова довіра в епоху дезінформації, та які рішення здатні забезпечити стійкість держави у новій реальності. Вказано, що в умовах гібридної війни кіберзахист є питанням стійкості всієї країни, тому має об’єднувати всі зацікавлені сторони – від держави та бізнесу до приватних ініціатив.* Текст: <https://fakty.ua/454081-cifrovaya-bezopasnost-trebuet-sotrudnichestva-na-vseh-urovnyah-itogi-infosec-ukraine-2025-v-kieve>
11. **Збірник тез Всеукраїнської науково-практичної конференції «Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення безпеки», (м. Київ, 27 вересня 2024 року)** / [редкол.: М. Г. Вербенський та ін.]. – Вінниця : Твори, 2024. – 406 с. : іл., табл. ***Шифр зберігання в Бібліотеці: А838016*** *Зі змісту:**Кібертероризм та проблеми кібербезпеки України в умовах воєнного стану / О. Зінченко. – С. 98-100; Оцінка ризиків поширення кіберзлочинів, пов’язаних із шахрайством / О. Користін (мол.). – С. 110-112; Кібербезпека в умовах гібридної війни: виклики та шляхи протидії / О. Лунгол. – С. 120-123; Використання злочинцями комп’ютерних систем та мереж / С. Демедюк. – С. 203-208; Протидія «комп’ютерним» злочинам в Україні: тренди та перспективи / М. Карчевський. – С. 215-220.*
12. **Здоровило Т. Добралися до ШІ: російські структури активізували методику «отруєння» великих мовних моделей** [Електронний ресурс] / Тарас Здоровило // Україна молода. – 2025. – 5 трав. – Електрон. дані. *Наведено коментар керівника Центру протидії дезінформації (ЦПД), офіцера Сил оборони України Андрія Коваленка щодо нових трендів у використанні РФ штучного інтелекту (ШІ) в інформаційній війні та на полі бою за останній місяць. Він відзначив, що на інформаційному фронті російські структури активізували методику «отруєння» великих мовних моделей (LLM), масово генеруючи фейкові сайти, новинні портали, псевдоаналітику через SEO-оптимізацію з метою спонукати різних ботів у відповідях мимоволі відтворювати кремлівські меседжі: про «нацистську Україну», «американську біозброю», «окупований Донбас» тощо. За словами посадовця, на полі бою скоро буде прорив у застосуванні автономних дронів: у США активно тестують дрони, які самостійно розпізнають ціль, ухвалюють рішення про атаку та виконують місію без участі людини. Своє чергою, ЦПД застосовує машинне навчання для виявлення координованих інформаційних атак: моделі фіксують аномалії в поширенні певного меседжу, одночасне підключення бот-мереж, «накачку» Telegram-каналів, інших соцмереж та реакції на них, внаслідок чого виявлена інфраструктура росіян поступово припиняє своє існування.* Текст: <https://umoloda.kyiv.ua/number/0/2006/189222/>
13. **Качуровська О. Британія почала готуватися до війни з РФ – ЗМІ** [Електронний ресурс] / Олена Качуровська // Korrespondent.net : [вебсайт]. – 2025. – 6 трав. – Електрон. дані. *Вказано, що Велика Британія таємно розпочала підготовку до прямого військового нападу з боку Росії через побоювання, що вона виявиться неготовою до війни. Як повідомило британське видання «The Telegraph», чиновникам доручили оновити 20-річні стратегії екстрених заходів, а також розробити новий план оборони країни. Засекречений документ включатиме питання захисту Кабінету міністрів і королівської сім'ї, а також громадське мовлення та накопичення ресурсів. У плані розглядаються сценарії, за яких країну атакують звичайними ракетами, ядерними боєголовками або за допомогою кібероперацій.* Текст: <https://ua.korrespondent.net/world/4778872-brytaniia-pochala-hotuvatysia-do-viiny-z-rf-zmi>
14. **Кметик Ю. Вибори президента в Румунії: російські хакери атакували сайти уряду** [Електронний ресурс] / Юлія Кметик // Focus.ua : [вебсайт]. – 2025. – 5 трав. – Електрон. дані. *Як повідомило румунське інформаційне агентство «G4media», 04.05.2025 російські хакери атакували сайти уряду Румунії та кандидатів у президенти, коли країна голосувала за свого наступного президента під час першого туру. Серед цілей зламників були сайти міністерств внутрішніх справ та юстиції Румунії. Йдеться про «NoName057» – проросійське хакерське угруповання, відоме серією кібератак на урядові вебсайти, медіа та приватні компанії в Україні, США та декількох країнах Європи. Група діє як вільна мережа цифрових активістів, метою яких є привернення уваги та поширення прокремлівського порядку денного на Заході.* Текст: <https://focus.ua/uk/digital/704733-vibori-prezidenta-v-rumuniji-rosiyski-hakeri-atakuvali-sayti-uryadu>
15. **Коба В. Б. Спосіб учинення кіберзлочинів як елемент криміналістичної характеристики: теоретична та практична проблематика** [Електронний ресурс] / Валерій Борисович Коба // Наук. перспективи. – 2025. – № 4. – С. 1156-1167. *Розглянуто деякі аспекти розслідування кіберзлочинів. Окреслено способи їх учинення. Зосереджено увагу на підготовчих заходах до вчинення кіберзлочинів та вказано на низку способів безпосереднього вчинення досліджуваної категорії протиправних діянь: шахрайські дії під час застосування електронно-обчислювальної техніки або (та) мережі Інтернет (фішинг, вішинг, кардінг); несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних систем, електронних комунікаційних мереж; умисне масове поширення повідомлень електрозв’язку, вчинене без попередньої згоди адресатів, яке мало наслідком порушення чи зупинення роботи електронно-обчислювальної техніки; злочинні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення; розповсюдження шкідливого програмного забезпечення або технічних засобів з використанням мережі Інтернет; збут шкідливого програмного забезпечення або технічних засобів із використанням мережі Інтернет.*  Текст: <http://perspectives.pp.ua/index.php/np/article/view/23221/23187>
16. **Красіков М. Космічна війна проти Росії: як удар по станції «Звезда» послабив розвідку РФ** [Електронний ресурс] / Максим Красіков // Focus.ua : [вебсайт]. – 2025. – 3 трав. – Електрон. дані. *Зазначено, що невідомі безпілотники вдарили по російському військовому об'єкту «Звезда» в Ставропольському краю РФ, що спеціалізується на космічній радіоелектронній розвідці, і є частиною стратегічної архітектури російської розвідки, яка використовується як для моніторингу ситуації у воєнних зонах, так і для підготовки інформації для інформаційно-психологічних операцій (ІПСО). Зокрема для кібершпигунства в Україні та у західних країнах. Вказано, що ця атака стала черговим епізодом у серії ударів по ключових елементах російської системи спостереження та протиповітряної оборони (ППО), демонструючи вразливість навіть найзасекреченіших об'єктів.*  Текст: <https://focus.ua/uk/eksklyuzivy/704556-kosmichna-viyna-yak-udar-po-stanciji-zvezda-poslabiv-rosiysku-rozvidku>
17. **Лаговська Н. В. Специфіка охорони програмного забезпечення в Україні: правовий аспект** [Електронний ресурс] / Н. В. Лаговська, О. В. Лаговський // Журн. східноєвроп. права : [електрон. наук.-практ. вид.] / ПВНЗ «Ун-т сучас. знань». – 2025. – № 133. – С. 130-136. *Досліджено правову охорону програмного забезпечення як об’єкта авторського права, зокрема правову природу комп’ютерних програм. Виявлено проблеми у чинному законодавстві щодо визначення авторства при колективній розробці, захисту прав розробників у відносинах з роботодавцями, боротьби з піратством та охорони прав у міжнародному контексті. Наголошено на необхідності удосконалення нормативно-правової бази та впровадження ефективних організаційно-правових механізмів. Запропоновано фіскальні та інвестиційні стимули для розвитку галузі ПЗ, яка є стратегічно важливою для національної економіки.* Текст: <http://easternlaw.com.ua/wp-content/uploads/2025/04/lagovska_lahovskyi_133.pdf>
18. **Лиса А. Союзники викрили масштабну кібероперацію ГРУ проти України** [Електронний ресурс] / А. Лиса // Korrespondent.net : [вебсайт]. – 2025. – 21 трав. – Електрон. дані. *Як повідомив Національний центр із питань кібербезпеки Великої Британії, у спільній заяві Великої Британії, США, Канади, Австралії, Польщі, Німеччини, Естонії й інших країн ідеться про викриття масштабної кібероперації, яку з 2022 р. вела військова частина 26165 ГРУ РФ. Кібершпигунська операція була спрямована на зрив логістики постачання західної зброї. Атаки спрямовувались проти організацій, що займаються координацією, транспортуванням і доставкою допомоги Україні, а також проти секторів оборони, ІТ-послуг, морського транспорту, аеропортів, портів і систем управління повітряним рухом у багатьох країнах-членах НАТО. Про масштаби кібератак та їхні наслідки поки не повідомляється*. Текст: <https://ua.korrespondent.net/world/4783686-souiznyky-vykryly-masshtabnu-kiberoperatsiui-hru-proty-ukrainy>
19. **Максимович Р. О. Кібербезпека в електронному врядуванні як запорука захисту персональних даних соціально вразливих верств населення** [Електронний ресурс] / Р. О. Максимович // Право та держ. упр.: зб. наук. пр. – 2024. – Вип. 4. – С. 312-317. *Розглянуто вплив розвитку цифрових технологій та електронного врядування на підвищення ефективності державного управління і доступності публічних послуг. Особливу увагу приділено проблемам кібербезпеки, зокрема захисту персональних даних громадян в умовах цифровізації. Проаналізовано основні загрози, серед яких – кібератаки, фішинг, злом баз даних, що особливо небезпечні для соціально вразливих груп населення. Обґрунтовано необхідність поєднання технічних, правових та освітніх заходів для підвищення рівня безпеки: вдосконалення інфраструктури захисту, розвиток цифрової грамотності, створення державних стратегій кіберзахисту. Підкреслено важливість підвищення контролю над збереженням даних та адаптації законодавства до нових викликів цифрового середовища.* Текст: <http://www.pdu-journal.kpu.zp.ua/archive/4_2024/43.pdf>
20. **Олександр Корнієнко: Без членства України в ЄС і НАТО бачення цілісної, вільної та мирної Європи залишиться неповним** [Електронний ресурс] / Прес-служба Апарату Верхов. Ради України // Голос України. – 2025. – 9 трав. (№ 343). – Електрон. дані.*Подано інформацію, що Перший заступник Голови Верховної Ради України (ВР України) провів робочу зустріч із делегацією Групи з міжпарламентських зв’язків з Україною Сеймасу Литовської Республіки на чолі із Саулюсом Лущикасом. У своєму виступі Олександр Корнієнко висловив глибоку вдячність Литві за її неоціненну підтримку України, яка триває протягом багатьох років, зокрема в контексті гібридної війни, що ведеться РФ проти України з 2014 р., включаючи військові, інформаційні, економічні та кібератаки. Він наголосив на важливості двосторонньої співпраці, підкресливши, що Литва завжди була надійним партнером і важливим союзником України в боротьбі на міжнародній арені, зокрема в контексті дипломатичної підтримки України на міжнародних форумах, санкційної політики проти РФ та підтримки європейської та євроатлантичної інтеграції України. Перший віцеспікер також підкреслив роль Литви як лідера у процесі регіональної співпраці, зазначивши, що її здатність об’єднувати Балтійсько-Скандинавські країни є надзвичайно важливою для України.* Текст: <https://www.golos.com.ua/article/383891>
21. **Орловський Б. М. Кримінологічний аналіз кіберзагроз та їх вплив на торгівельне мореплавство** [Електронний ресурс] / Б. М. Орловський, І. А. Осадча // Прав. держава / Одес. нац. ун-т ім. І. І. Мечникова. – 2025. – № 57. – С. 263-273. *Здійснено кримінологічне дослідження кіберзагроз та їх впливу на кібербезпеку у сфері торгівельного мореплавства. Кіберзагрози визначено як сукупність негативних чинників, факторів або явищ, що за напрямком свого впливу спрямовані на пошкодження інформаційних, телекомунікаційних та інших систем, які забезпечують належне функціонування діяльності підприємств, установ, організацій або держави та захист інформації у таких системах. Виділено складові елементи кіберзагроз у сфері торгівельного мореплавства та проаналізовано міжнародно-правове регулювання кіберзагроз, що охоплюється «Міжнародним кодексом з охорони суден і портових засобів» (ISPS Code), «Керівництвом з управління морськими кіберризиками», «Керівництвом (Рекомендаціями) з кібербезпеки на борту суден» тощо. Розглянуто детермінанти та мотивацію кіберзлочинців у цій сфері (фінансовий аспект, усунення конкурентів, мотиви помсти, ідеологічні мотиви) та сформульовано ключові заходи задля профілактики та запобігання кіберзагроз у сфері торгівельного мореплавства.*  Текст: <http://pd.onu.edu.ua/article/view/325403/317574>
22. **Савін Т. «Працюють з «Акваріума»: у РФ створили нову спецслужбу для війни із Заходом, – The Sun** [Електронний ресурс] / Тимур Савін // Focus.ua : [вебсайт]. – 2025. – 12 трав. – Електрон. дані. *Йдеться про секретну структуру «КДБ 2.0», що виконує завдання з кібератак і вбивств у Європі. Вказано, що російські агенти стоять за замахом на гендиректора німецького військового гіганта «Rheinmetall» А. Паппергера. Західні розвідники стверджують, що ця тіньова організація називається «Департамент спеціальних завдань» (ДСЗ) – новий інструмент Москви в гібридній війні проти Заходу, що діє з «Акваріума», відомої штаб-квартири ГРУ в Москві. На думку експертів, ДСЗ створили 2023 р. в розпал війни в Україні. Зазначено, що діяльність структури охоплює спроби організації терактів, убивства та кібератаки для виведення західних держав із рівноваги.* Текст: <https://focus.ua/uk/politics/705699-pracyuyut-z-akvariuma-u-rf-stvorili-novu-specsluzhbu-dlya-viyni-iz-zahodom-the-sun>
23. **Савін Т. РФ готує масштабну кібератаку: постраждає логістика військової допомоги для України, – Reuters** [Електронний ресурс] / Тимур Савін // Focus.ua : [вебсайт]. – 2025. – 21 трав. – Електрон. дані. *Як повідомило агентство «Reuters», західні логістичні структури і технологічні компанії, які надають військову допомогу Україні, стануть метою кібератаки російських хакерів. Велика Британія і США попередили про це Україну і союзників. Зазначено, що кібератака РФ буде націлена на сектори оборони, ІТ-послуг, морського судноплавства, аеропорти і системи управління повітряним рухом у багатьох країнах НАТО.* Текст: <https://focus.ua/uk/digital/707234-rosiya-gotuye-masshtabnu-kiberataku-golovni-cili>
24. **Савінцев С. Російські хакери з ГРУ атакували логістику
13 держав НАТО: цікавили поставки Україні** [Електронний ресурс] / Сергій Савінцев // Focus.ua : [вебсайт]. – 2025. – 22 трав. – Електрон. дані. *Зазначено, що група хакерів, яких фінансувала РФ, починаючи з 2022 р., атакувала щонайменше 13 держав членів НАТО та Україну, аби отримати інформацію про постачання західного озброєння Києву. Про це йдеться в аналітичному звіті агентства кібербезпеки та захисту інфраструктури (CISA) Департаменту внутрішньої безпеки США. Вказано, що основними цілями кампанії стали логістичні компанії, ІТ-підприємства та транспортна інфраструктура, що забезпечують координацію, транспортування та доставку іноземної допомоги Україні. Російські хакери атакували компанії, пов'язані з оборонною промисловістю, транспортом і транспортними вузлами (портами, аеропортами тощо), морською галуззю, управлінням повітряним рухом, ІТ-послугами. У звіті зазначено, що було захоплено тисячі IP-камер на прикордонних пунктах пропуску та залізничних вузлах, що дало російській розвідці можливість у режимі реального часу спостерігати за колонами гуманітарної допомоги*. Текст: <https://focus.ua/uk/digital/707258-rosiyski-hakeri-z-gru-atakuvali-logistiku-13-derzhav-nato-cikavili-postavki-ukrajini>
25. **Семеренко І. Заразили понад 300 тисяч пристроїв: у The Guardian розкрили деталі масштабної кібератаки РФ** [Електронний ресурс] / Ірина Семеренко // Focus.ua : [вебсайт]. – 2025. – 24 трав. – Електрон. дані. *Про деталі російської кібератаки повідомили у «The Guardian». Зазначено, що російські хакери проникли у понад 300 000 комп'ютерів по всьому світу. Метою масштабної кібератаки стало викрадення даних, шантаж, а також кібершпигунство проти урядових, дипломатичних і військових установ. Слідчі виявили 37 злочинців, серед них – громадянин РФ В. Ковальов, якого називають одним із найбільш розшукуваних зловмисників німецьким агентством боротьби зі злочинністю «Bundeskriminalamt» («BKA»).*  Текст: <https://focus.ua/uk/digital/707577-zarazili-ponad-300-tisyach-pristrojiv-u-the-guardian-rozkrili-detali-masshtabnoji-kiberataki-rf>
26. **Семеренко І. Партизани в Криму здійснили кібератаку на кремлівські сайти і зламали телефон командира ППО** [Електронний ресурс] / Ірина Семеренко // Focus.ua : [вебсайт]. – 2025. – 11 трав. – Електрон. дані. *Зазначено, що партизанам вдалося вивести з ладу два ключових кремлівських медіаресурси в Криму: це сайти, що є головними рупорами російської пропаганди на території тимчасово окупованого півострова. Також їм вдалося зламати телефон командира сил протиповітряної оборони (ППО), який відповідає за російські військові об'єкти в Криму*. Текст: <https://focus.ua/uk/voennye-novosti/705635-partizani-v-krimu-kiberfahivci-viveli-z-ladu-klyuchovi-sayti-rosiyskoji-propagandi>
27. **Ситняк В. В Україні ФСБ РФ вербує молодь: як діяти у випадку отримання повідомлення (відео)** [Електронний ресурс] / Вікторія Ситняк // Focus.ua : [вебсайт]. – 2025. – 16 трав. – Електрон. дані. *Йдеться про те, що в Україні триває масове вербування російськими спецслужбами через інтернет. За даними Центру стратегічних комунікацій та інформаційної безпеки, 22 % завербованих – діти віком до 18 років, яких використовують як витратний матеріал. Зазначено, що проблема вербування набула масштабів національної загрози. Служба безпеки України (СБУ) зафіксувала понад 600 випадків, коли українців намагалися втягнути в диверсійні дії проти своїх же співгромадян. Центр стратегічних комунікацій та інформаційної безпеки повідомив, що робити у випадку виходу на контакт ФСБ РФ.* Текст: <https://focus.ua/uk/voennye-novosti/706518-v-ukrajini-fsb-rf-verbuye-molod-yak-diyati-u-vipadku-otrimannya-povidomlennya-video>
28. **Сперкач Н. А. Кримінологічні заходи запобігання кримінальним правопорушенням у сфері інформаційних технологій та шляхи їх вдосконалення** [Електронний ресурс] / Н. А. Сперкач, І. В. Кибиш / Аналіт.-порівнял. правознавство : електрон. наук. вид. – 2025. – № 1. – С. 658-663. *Проведено комплексне дослідження історичних аспектів процедур із запобігання кримінальним правопорушенням у сфері використання інформаційних технологій (ІТ). Проаналізовано сучасні міжнародні стандарти у цій галузі, розкрито загально-соціальні засади запобігання таким кримінальним правопорушенням. Увагу приділено процесу формування спеціально-кримінологічних заходів запобігання на сучасному етапі кримінальним правопорушенням, що вчиняються з використанням ІТ; надано пропозиції щодо індивідуальних підходів до запобігання кримінальним правопорушенням у цій сфері.* Текст: <https://app-journal.in.ua/wp-content/uploads/2025/02/111.pdf>
29. **Технологія OSINT в управлінні кризовими ситуаціями та попередженні кіберзагроз** : наук.-практ. посіб. / Олександр Довгань, Артем Старосєк, Анатолій Тарасюк, Тарас Ткачук ; Держ. наук. установа «Ін-т інформації, безпеки і права НАПН України». – Київ ; Одеса : Фенікс, 2024. – 183 с. : іл., табл. ***Шифр зберігання в Бібліотеці: А838160*** *Досліджено інструменти та методи добування й опрацювання військової, політичної, економічної та іншої інформації з відкритих джерел з метою її подальшого аналізу та використання для прийняття рішень у сфері національної безпеки і оборони, проведення розслідувань тощо. Розглянуто специфіку роботи з протидії ворожим маніпулятивним впливам в інформаційному просторі, яка базується на методах OSINT і здійснюється в інтересах реалізації стратегічного наративу держави. Викладено узагальнені підходи до аналізу відкритих джерел інформації та обґрунтовано критерії, що висуваються до даних, отриманих із таких джерел. Узагальнені критерії дали можливість визначити перелік програмних продуктів, які доцільно використовувати при проведенні OSINT; надано їх стислий огляд і можливості.*
30. **Топчій В. В. Проблемні питання забезпечення кібербезпеки в Україні** [Електронний ресурс] / В. В., Топчій О. М. Бодунова / Аналіт.-порівнял. правознавство : електрон. наук. вид. – 2025. – № 1. – С. 664-669. *Вивчено та узагальнено проблемні аспекти забезпечення кібербезпеки в Україні під час воєнного стану та визначено можливі напрями їх усунення. Доведено, що для того, щоб комплексно вирішувати питання запобігання злочинності у сфері кіберзлочинності, Україні потрібно ввести додаткові нормативно-правові акти, що будуть орієнтовані не лише на реагування на кіберзагрози, але й на більш ефективне запобігання кіберзлочинності. Вказано на необхідність впровадження відповідальності за вищезазначені кримінальні правопорушення, вчинені під час воєнного стану. Підкреслено, що особа, яка завдає шкоди національним інтересам України у кіберпросторі й у такий спосіб допомагає агресору в цій війні, повинна нести відповідальність аналогічно воєнним злочинцям.* Текст:<https://app-journal.in.ua/wp-content/uploads/2025/02/112.pdf>
31. **Трофименко В. Кіберпростір і держава: точки перетинання** [Електронний ресурс] / Володимир Трофименко // Вісн. НЮУ ім. Ярослава Мудрого. Серія : Філософія, філософія права, політологія, соціологія : зб. наук пр. – Харків, 2024. – Т. 4 (№ 63). – С. 116-129. *Проаналізовано основні підходи держави до кіберпростору: класичного – з позицій традиційної науки та нового – з позицій тлумачення кіберпростору як особливої сфери регулювання. Виділено три основних перспективних напрямки взаємодії держави та кіберпростору: технічний, політичний та економічний. Акцентовано на тому, що, незважаючи на існуючі нормативні прогалини, лише держава здатна провести певне регулювання існуючих відносин не тільки за наведеними, а і в інших сферах кіберпростору.* Текст: <http://fil.nlu.edu.ua/article/view/315212>
32. **Управління системами захисту інформації та кібернетичної безпеки** / [В. М. Тупкало та ін.] ; за ред. В. М. Тупкало, В. І. Богом’ї ; М-во освіти і науки України, Київ. ун-т інтелект. власності та права Нац. ун-ту «Одес. юрид. акад.». – Київ : Людмила, 2025. – 231 с. : іл., табл. ***Шифр зберігання в Бібліотеці: В84353*** *У монографії об’єктами дослідження є об’єкти критичної інфраструктури підприємств та установ, включаючи комп’ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні ресурси і технології забезпечення безпеки інформації. Проаналізовано процеси управління інформаційною та/або кібернетичною безпекою об’єктів, що підлягають захисту, а також методи розслідування інцидентів, управління ризиками та методики захисту від негативного інформаційного впливу тощо.*
33. **Уткіна М. Цифрові технології: виклик чи можливість для протидії фінансовій злочинності?** [Електронний ресурс] / М. Уткіна // Юрид. вісн. – 2025. – № 1. — С. 155-162. *Розглянуто цифровізацію фінансового сектора через призму нових можливостей у сфері протидії фінансовій злочинності. Висвітлено роль цифрових технологій у системі протидії фінансовій злочинності. Проаналізовано питання їх нормативно-правового регулювання, а також окреслено виклики, які постають перед правоохоронними органами, фінансовими інституціями та державними регуляторами. Зосереджено увагу на впливі цифровізації на механізми запобігання й розслідування фінансових злочинів, зокрема на використанні штучного інтелекту (ШІ), технологій аналізу великих даних (Big Data) й блокчейну. Акцентовано на питаннях кібербезпеки у фінансовій сфері, включаючи правові аспекти застосування біометричних технологій, багаторівневої аутентифікації та систем моніторингу транзакцій у режимі реального часу. Зроблено висновок, що цифрові технології є не лише ефективним інструментом протидії фінансовим злочинам, а й потенційним джерелом формування нових загроз, зумовлюючи необхідність адаптації правових механізмів до сучасних умов цифрової трансформації фінансового сектору.* Текст: <http://yurvisnyk.in.ua/v1_2025/22.pdf>
34. **Христюк В. В. Поняття та кваліфікаційні ознаки кримінального правопорушення «кіберексплуатація людини»** [Електронний ресурс] / В. В. Христюк // Юрид. наук. електрон. журн. – 2025. – № 3. – С. 378-381. *Розглянуто поняття та кваліфікаційні ознаки такого кримінального правопорушення як «кіберексплуатація людини», що виступає як специфічна форма кримінального правопорушення у сфері незаконної експлуатації людини. Виявлено та систематизовано особливості цього кримінального правопорушення у сфері експлуатації людини в умовах інформаційного суспільства. Розроблено рекомендації щодо його правової кваліфікації та правозастосування. Проаналізовано національне законодавство, судову практику та міжнародні стандарти у сфері прав людини та боротьби з кіберзлочинністю. Запропоновано поняття «кіберексплуатація людини» та здійснено порівняння таких понять як «кібербулінг», «онлайн-експлуатація», «кібершахрайство». Кіберексплуатацію людини визначено як протиправне використання особи з метою отримання незаконної вигоди або заподіяння шкоди, вчинене за допомогою інформаційно-комунікаційних технологій. Окреслено основні кваліфікаційні ознаки цього злочину, а саме: використання інформаційних технологій для залучення, контролю або експлуатації особи; наявність прямого умислу щодо отримання вигоди; порушення прав і свобод людини. Зроблено висновок про важливість вдосконалення національних норм і міжнародних стандартів, які регулюють цю сферу, з метою забезпечення ефективної боротьби з кіберзлочинністю та захисту прав людини в умовах глобалізації.* Текст: <http://www.lsej.org.ua/3_2025/91.pdf>
35. **Шевчук М. О. Поняття суб'єкта інформаційної безпеки** [Електронний ресурс] / М О. Шевчук // Право та держ. упр.: зб. наук. пр. – 2024. – Вип. 4. – С. 90-98. *Досліджено поняття суб'єкта інформаційної безпеки та його роль у захисті інформаційного простору. Виокремлено три основні суб'єкти: суспільство, державу та особу (фізичну і юридичну), проаналізовано їхні функції, взаємодію та реагування на загрози. Наголошено на необхідності координації між усіма сторонами, особливо за участі приватного сектора, для ефективного забезпечення кібербезпеки. Надано рекомендації щодо покращання співпраці задля зміцнення національної інформаційної безпеки.* Текст: <http://www.pdu-journal.kpu.zp.ua/archive/4_2024/14.pdf>
36. **Шпак І. У Росії 9 травня масово вимикають інтернет: обмеження охоплять 60 % території країни, – росЗМІ** [Електронний ресурс] / Ірина Шпак // Focus.ua : [вебсайт]. – 2025. – 8 трав. – Електрон. дані. *Зазначено, що вперше в новітній історії РФ влада запровадить масштабні обмеження мобільного інтернету – доступ буде суттєво обмежено на понад 60 % території країни, переважно в її європейській частині. Відповідне рішення ухвалила Рада безпеки РФ, а впроваджуватиме його Роскомнадзор. Нові обмеження почнуть діяти вже 09.05.2025. Вказано, що IT-експерти називають це рішення безпрецедентним і попереджають про серйозні перебої в роботі ключових цифрових сервісів. Наголошено, що за умов, коли в сучасній РФ багато сфер життя – від онлайн-торгівлі до логістики – залежать від стабільного інтернету, такі обмеження можуть спричинити справжній колапс.* Текст: <https://focus.ua/uk/world/705365-rosiya-obmezhuye-mobilniy-internet-9-travnya-shcho-vidomo-pro-masshtabni-vidklyuchennya-zv-yazku>

**Підготовлено відділом інформаційного забезпечення органів влади**

**Національної бібліотеки України імені Ярослава Мудрого**

**Відповідальний за випуск: Зайченко Н. Я.**

**31.05.2025**