**Кібербезпека**

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

***анотований бібліографічний список***

***2025. – Вип. 7 (липень). – 11 с.***

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

1. **Бережна Д. Не тільки «Аерофлот»: хакери обрушили в РФ мережу аптек й отримали дані тисяч росіян** [Електронний ресурс] / Дар’я Бережна // Focus.ua : [вебсайт]. – 2025. – 29 лип. – Електрон. дані. *Як повідомило російське видання «The Moscow Times», у Москві та регіонах зупинили роботу аптеки холдингу «Неофарм»: йому належить понад
1000 точок у 80 містах у центральній Росії. Вказано, що наразі недоступні бронювання ліків, також не працюють каси і системи обліку, а працівників відправили у відгул. Також повідомлено, але не афішується, що хакери з «Silent Crow», ті самі, що взяли на себе відповідальність за злом «Аерофлоту», заявили про злом «Єдиної медичної інформаційно-аналітичної системи» і крадіжку 17 ТБ медичних даних москвичів. Хакери заявили, що внаслідок успішної операції отримали повний доступ до мережі, яка обслуговує мешканців Москви і Московської області, а також отримали адміністративний контроль над усією інфраструктурою одного з найбільших «операторів персональних даних», включно з доменом контролером, гіпервізорами, базами даних*. Текст: <https://focus.ua/uk/digital/716760-ne-tilki-aeroflot-hakeri-obrushili-v-rf-merezhu-aptek-i-rozdobuli-dani-tisyach-rosiyan>
2. **Бибик Д. Д. Кібербезпека в системі сучасної вищої освіти : реалії та перспективи подальшого розвитку** [Електронний ресурс] / Д. Д. Бибик, С. І. Тополянський // Наук. вісн. Ужгород. нац. ун-ту. Серія : Педагогіка. Соц. робота. – 2025. – № 1 (56). – С. 45-50. *Метою дослідження є аналіз загроз кіберзлочинності в освіті та розробка пріоритетних заходів для їх запобігання. Вказано, що ключовими факторами успішного забезпечення кібербезпеки є рівень підготовки учасників освітнього процесу, їхня відповідальність і професійні навички, а також ефективність функціонування освітніх платформ. Запропоновано заходи, які включають удосконалення політики кіберзахисту, підвищення цифрової грамотності, кіберобізнаності та впровадження національної стратегії кібербезпеки, що сприятиме стабільному функціонуванню закладів вищої освіти(ЗВО) та зменшенню ризиків кіберзагроз.* Текст : <http://visnyk-ped.uzhnu.edu.ua/article/view/329986>
3. **Вовк А. Сучасні проблеми публічного управління забезпеченням кібербезпеки в Україні** [Електронний ресурс] / Артем Вовк // Публіч. упр. : концепції, парадигма, розвиток, удосконалення. – 2024. – № 8. –
С. 28-35. *Систематизовано наукові дослідження сучасних проблем публічного управління у сфері кібербезпеки в Україні. Визначено кібербезпеку як захист комп’ютеризованих систем від несанкціонованого доступу та загроз. Проаналізовано сучасні виклики, зокрема постійне оновлення кіберзагроз, високі ризики у фінансовому секторі та загрози витоку персональних даних органів влади. Виокремлено інноваційні підходи до забезпечення кібербезпеки, такі як розвідка загроз, машинне навчання, архітектура нульової довіри та управління ризиками. Окреслено напрями вдосконалення публічного управління: впровадження новітніх технологій захисту, розвиток кадрового потенціалу, вдосконалення нормативно-правової бази, активізація міжнародного співробітництва, а також проведення комплексних наукових досліджень. Акцентовано на необхідності скоординованих дій усіх суб’єктів кібербезпеки для ефективної протидії кіберзагрозам.*  Текст: <https://pa.journal.in.ua/index.php/pa/article/view/136>
4. **Гал І. Хакери зламали систему безпеки російського «Аерофлоту»: йдеться про повне знищення IT-інфраструктури компанії** [Електронний ресурс] / Ірина Гал // Fakty.ua : [вебсайт]. – 2025. – 28 лип. – Електрон. дані. *Йдеться про хакерську атаку, яка «поклала» російський «Аерофлот». Російський перевізник повідомив про «збій в інформаційних системах авіакомпанії» та «вимушене коригування розкладів рейсів, у тому числі шляхом переносу чи скасування». Наразі повідомлено про скасування більше ніж 40 рейсів із Москви. Як повідомив ресурс «Nexta», відповідальність за атаку на «Аерофлот» взяли на себе угруповання «Silent Crow» та «Кіберпартизани Білорусі». Хакери зазначили, що операція тривала рік і завершилася повним крахом внутрішньої ІТ-системи авіагіганта: знищено близько 7000 серверів, викрадено 20 Тб даних. Зауважено, що в результаті атаки було отримано доступ, зокрема, до корпоративної пошти «Аерофлоту» та внутрішніх документів, а збитки від атаки можуть обчислюватися десятками мільйонів доларів.* Текст: <https://fakty.ua/457646-hakery-vzlomali-sistemu-bezopasnosti-rossijskogo-quot-aeroflota-quot-rech-idet-o-polnom-unichtozhenii-it-infrastruktury-kompanii>
5. **Денисова Д. Коли смартфон небезпечний: як врятувати свої рахунки і гроші від кібершахраїв** [Електронний ресурс] / Дар'я Денисова // Focus.ua : [вебсайт]. – 2025. – 28 лип. – Електрон. дані. *Зазначено, що шахрайство набуло нових форм, де головною зброєю зловмисників стала не техніка, а психологія: аферисти адаптуються до нових технологій, використовуючи соціальну інженерію, штучний інтелект (ШІ) та емоційні маніпуляції. Вказано, що понад 83 % усіх шахрайських операцій в Україні за рік відбулося в інтернеті. За даними Національного банку України (НБУ), саме онлайн-шахрайство спричинило 93 % загальної суми збитків, а середня сума однієї незаконної операції зросла на 51 % — до 4761 грн. Розглянуто найпоширеніші схеми шахрайських операцій з картками і як в такій ситуації захистити свої гроші.*  Текст: <https://focus.ua/uk/economics/716467-shahraystvo-v-interneti-ta-cherez-gadzheti-nayposhirenishi-shemi-i-pastki>
6. **Денисова Д. Топ-5 схем, як шахраї крадуть гроші з карткових рахунків** [Електронний ресурс] / Дар'я Денисова // Focus.ua : [вебсайт]. – 2025. – 28 лип. – Електрон. дані. *Йдеться про те, що інтернет-шахрайство вже давно перестало бути примітивним явищем – сьогодні це складні, технологічно витончені атаки, що ґрунтуються на детальному аналізі поведінки користувачів. Як повідомила юристка М. Кузьменко, серед найбільш поширених схем інтернет-шахрайства, а також тих, які найскладніше виявити, вирізняються фішинг і його варіації. За її словами, це одна з наймасовіших форм атак, яка передбачає отримання персональних даних. Розглянуто всі найпоширеніші схеми шахрайських операцій з картками. Серед них: deepfake-відео та голосове шахрайство, смс- і месенджер-шахрайство, фішинг та його варіації, шахрайські застосунки та фейкові оновлення, підміна контактів і повідомлень. Вказано, чи є шанс повернути гроші і спіймати інтернет-шахрая*. *Як зазначила фахівчиня, в Україні фішинг та інші форми онлайн-шахрайства кваліфікують за декількома статтями Кримінального кодексу України (КК України), серед яких ст. 190 КК України – шахрайство; ст. 209 КК України – легалізація (відмивання) доходів, одержаних злочинним шляхом тощо. Вказано, що розслідування інтернет-шахрайства в Україні здійснюють кілька уповноважених органів. Основним є Кіберполіція України – спеціалізований підрозділ Національної поліції України, який займається виявленням, документуванням і припиненням кіберзлочинів, зокрема пов’язаних із шахрайством в Інтернеті.* Текст: <https://focus.ua/uk/economics/716480-nayposhirenishi-shemi-internet-shahraystva-yurist-rozpoviv-yak-zahistitisya>
7. **Добров В. Маніпулятивна журналістика: політтехнолог розповів, як в Україні працюють схеми інфоздирництва** [Електронний ресурс] / Володимир Добров // Fakty.ua : [вебсайт]. – 2025. – 8 лип. – Електрон. дані. *Зазначено, що в Україні роками існує тіньовий ринок інформаційного шантажу під прикриттям псевдорозслідувань. Як повідомило видання «Головне в Україні» виконавчий директор Агентства моделювання ситуацій Олексій Голобуцький на своїй сторінці у «Facebook» розповів про схеми тиску, які використовують окремі медіаресурси задля збагачення, маніпулюючи репутаціями компаній та підприємців. За словами політтехнолога, найяскравішим прикладом такої схеми є сайт «Антикор», який під виглядом «антикорупційного порталу» розміщує сумнівні матеріали, що часто містять перекручені або фейкові дані. Після цього представники ресурсу пропонують видалити контент — за гроші. Як зазначив експерт, ціна такого «очищення» стартує з кількох тисяч доларів і може сягати десятків тисяч. Якщо пропозицію ігнорують — публікацію множать на десятках «дзеркальних» сайтів і телеграм-каналів: така тактика створює ілюзію суспільного резонансу і спричиняє реальні репутаційні збитки для компаній та підприємців. У прикладах, наведених О. Голобуцьким, фігурують як великі українські бренди, так і міжнародні компанії, які стикалися з шантажем і подавали судові позови. Деякі виграли справи, але більшість постраждалих змушені нести репутаційні втрати без реального захисту з боку держави*. Текст: <https://fakty.ua/456765-manipulyativnaya-zhurnalistika-polittehnolog-rasskazal-kak-v-ukraine-rabotayut-shemy-infovymogatelstva>
8. **Купновицька У. Збій Starlink: як кілька годин без звʼязку змінили ситуацію на передовій** [Електронний ресурс] / Уляна Купновицька // Focus.ua : [вебсайт]. – 2025. – 25 лип. – Електрон. дані. *Зазначено, що у ніч на 25 липня українські військові зіткнулися з несподіваною проблемою – десятки терміналів «Starlink» раптово вийшли з ладу, зв’язок зник на ключових ділянках фронту, включно з найгарячішими напрямками – Харківським, Донбаським і Запорізьким. Вказано, що про глобальний збій першими повідомили військові з підрозділів, що активно використовують «Starlink» для координації дронів, передачі розвідданих та зв’язку між підрозділами. Техніка просто відмовилася працювати: пристрої або не підключалися до мережі, або миттєво втрачали сигнал. Зауважено, що проблема виявилася не локальною – схожі збої фіксуються і в інших країнах: США, Франції, Польщі та Новій Зеландії. На сайті «DownDetector» пік скарг припав саме на ніч проти 25 липня. «Фокус» розбирався, чи має Україна альтернативу «Starlink» і чому небезпечно залежати від однієї системи зв’язку*. Текст: <https://focus.ua/uk/eksklyuzivy/716179-zbiy-starlink-na-fronti-chim-ce-zagrozhuye-ukrajini-ta-chi-ye-alternativa>
9. **Митропан А. Як сьогодні працюють кібершахраї в українському бізнес-середовищі** [Електронний ресурс] / Анна Митропан // Юрид. газ. – 2025. – 16 лип. – Електрон. дані. *За словами автора статті, у період повномасштабної війни Україна стала ареною зростання кіберзлочинності. З 2022 до 2025 р. українські компанії – державні та приватні – стали мішенями різноманітних кібератак, від DDoS до програм-руйнівників. Проаналізовано реальні кейси з кіберінцидентами, методи кібершахраїв та юридичні наслідки їхньої діяльності в Україні. Наведено приклади кібератак на українські бізнеси. Розглянуто особливості та проблеми покарання кіберзлочинців.* Текст: <https://yur-gazeta.com/dumka-eksperta/yak-sogodni-pracyuyut-kibershahrayi-v-ukrayinskomu-biznesseredovishchi.html>
10. **Мозговий І. Хакери ГУР зламали «Газпром»: подробиці масштабної кібероперації** [Електронний ресурс] / Іван Мозговий // Fakty.ua : [вебсайт]. – 2025. – 19 лип. – Електрон. дані. *Як повідомило «Суспільне», українські кіберфахівці здійснили успішну атаку на ІТ-інфраструктуру російської корпорації «Газпром». За інформацією джерел у розвідці, операція Головного управління розвідки Міністерства оборони України (ГУР МО України) призвела до знищення інформаційної системи компанії. За оцінками ГУР, кібератака суттєво зменшить доходи російського бюджету. Вказано, що кіберфахівці отримали повний доступ до всіх інформсистем компанії, скопіювали сотні терабайт даних, включаючи інформацію про
20 тис. співробітників компанії та бази даних 390 дочірніх компаній та філій «Газпрому». Після цього всі дані, включаючи резервні копії, були повністю видалені з фізичних і хмарних серверів.* Текст: <https://fakty.ua/457279-hakery-gur-vzlomali-gazprom-podrobnosti-masshtabnoj-kiberoperacii>
11. **Національна безпека та оборонна політика** : навч. посіб. [для використання у навч.-вихов. процесі / В. М. Телелим та ін. ; за заг. ред. М. В. Коваля] ; Нац. ун-т оборони України. – Київ : НУОУ, 2024. – 318 с. ***Шифр зберігання в Бібліотеці:*** ***А838577*** *Розглянуто питання національної, воєнної, економічної, інформаційної безпеки держави, кібербезпеки та прогнозування розвитку безпекового середовища.*
12. **Носальська І. Системна робота: очікувані наслідки від знищення логістики РФ** [Електронний ресурс] / Ірина Носальська // Korrespondent.net : [вебсайт]. – 2025. – 31 лип. – Електрон. дані. *Йдеться про масштабну атаку хакерів із угруповань «Silent Crow» і «Кіберпартизани BY» на російський «Аерофлот», унаслідок якої відбулось повне знищення його
IT-інфраструктури. Наголошено, що завдані РФ збитки від цієї кібератаки є стратегічним, а відновлення роботи компанії вимагатиме десятки мільйонів доларів. За словами експертів, провал і колапс «Аерофлоту» означає провал і колапс всього авіасполучення у РФ, тому що це стрижнева, базова авіакомпанія країни-агресорки: була зупинена не тільки її робота, але і багатьох аеропортів, котрі значною мірою підживлювалися «айтішно» від «Аерофлоту». Акцентовано також на системних атаках українських безпілотників по російській залізниці, мета яких – уповільнити залізничний рух і вивести з ладу логістику РФ. І якщо раніше Сили оборони України активно атакували залізничні потяги в окупованій частини Запорізької області, то зараз регулярні удари БПЛА по залізницях перемістилися на південь РФ*. Текст: [https://ua.korrespondent.net/articles/4803990-systemna-robota-ochikuvani-naslidky-vid-znyschennia-lohistyky-rf?\_gl=1\*1l6ivnh\*\_gcl\_au\*ODAzMjUxMzcxLjE3NDcyNTQ5NTA.\*\_ga\*MTQ0ODc1MjAyMC4xNzIwNDY2NDU5\*\_ga\_HCSJ3J3LKX\*czE3NTM5ODI4ODgkbzgyMyRnMSR0MTc1Mzk4NDEwOSRqNjAkbDAkaDk4NTY1OTAwNQ](https://ua.korrespondent.net/articles/4803990-systemna-robota-ochikuvani-naslidky-vid-znyschennia-lohistyky-rf?_gl=1*1l6ivnh*_gcl_au*ODAzMjUxMzcxLjE3NDcyNTQ5NTA.*_ga*MTQ0ODc1MjAyMC4xNzIwNDY2NDU5*_ga_HCSJ3J3LKX*czE3NTM5ODI4ODgkbzgyMyRnMSR0MTc1Mzk4NDEwOSRqNjAkbDAkaDk4NTY1OTAwNQ)
13. **Поетапне впровадження моделі, заснованої на профілях безпеки, має на меті значно спростити адміністративні процедури** [Електронний ресурс] / Прес-служба Апарату Верхов. Ради України // Голос України. – 2025. – 12 лип. (№ 388). – Електрон. дані. *Як повідомили у Комітеті Верховної Ради України (ВР України) з питань цифрової трансформації, Державна служба спеціального зв’язку та захисту інформації України зробила черговий важливий крок на шляху реформування системи кіберзахисту. Наказами адміністрації Держспецзв’язку затверджено базові профілі безпеки для інформаційних, електронних комунікаційних, інформаційно-комунікаційних і технологічних систем, де обробляється відкрита, конфіденційна, службова інформація. Зазначено, що документи встановлюють мінімальні вимоги з безпеки інформації та є фундаментальними елементами у переході від класичної моделі побудови комплексних систем захисту інформації (КСЗІ) до гнучкого та адаптивного підходу, що ґрунтується на профілях безпеки.* Текст: <https://www.golos.com.ua/article/385151>
14. **Прокопенко Н. М. Поняття та кримінально-правова характеристика торгівлі людьми у кіберсфері** [Електронний ресурс] / Н. М.Прокопенко// Наук. вісн. публіч. та приват. права. – 2025. – № 1. – С. 161-167. *Проаналізовано поняття та надано кримінально-правову характеристику торгівлі людьми в кіберпросторі з урахуванням сучасних тенденцій розвитку міжнародних стандартів, цифрового середовища та національного законодавства України. Окреслено основні форми цього злочину, які можуть виникати у зв’язку із цифровими технологіями (соціальні мережі, даркнет і криптовалюта), застосування яких ускладнює процес для виявлення та припинення таких злочинів. Особливу увагу приділено правовим аспектам боротьби з кіберторгівлею людьми, акцентовано на кримінальній відповідальності за торгівлю людьми в Україні відповідно до Кримінального кодексу (КК України). Розглянуто міжнародно-правові механізми та конвенції, спрямовані на виявлення та боротьбу з торгівлею людьми. Надано пропозиції щодо посилення боротьби з означеним злочином, серед яких: вдосконалення законодавства; активізація міжнародного співробітництва; підготовка фахівців, здатних працювати у сфері кібербезпеки та кримінальної юстиції.* Текст: <http://nvppp.in.ua/vip/2025/1/30.pdf>
15. **Рогозіннікова К. С. Роль Служби безпеки України у забезпеченні кібербезпеки держави в умовах воєнного стану** [Електронний ресурс] / К. С. Рогозіннікова // Наук. вісн. публіч. та приват. права. – 2025. –
№ 1. – С. 123-128. *Розглянуто діяльність СБУ у сфері забезпечення кібербезпеки України в умовах повномасштабної війни Росії проти України. Проаналізовано нормативно-правові акти, якими забезпечується важливий функціонал СБУ та її підрозділів у галузі кібербезпеки. Виокремлено ключові аспекти, які необхідно удосконалити з урахуванням викликів сучасних кіберзагроз. Наведено приклади реальної військової кіберагресії, спрямованої проти України, та розглянуто роль Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ у запобіганні та нейтралізації таких загроз. Вказано на необхідність злагодженого функціонування європейської системи кібербезпеки та доцільність створення європейської кіберкоаліції як механізму колективного реагування на масштабні кіберзагрози. Акцентовано на ролі СБУ як одного з ключових суб’єктів не лише національної системи кіберзахисту, а й загалом всієї національної безпеки.* Текст: <http://www.nvppp.in.ua/vip/2025/1/24.pdf>
16. **Синицін М. Три найнебезпечніші схеми кібершахрайства в Україні: як обманюють і чи є засоби захисту** [Електронний ресурс] / Микита Синицін // Fakty.ua : [вебсайт]. – 2025. – 11 лип. – Електрон. дані. *Йдеться про те, що онлайн-шахрайство в Україні нарощує масштаби, тож українців навіть просять відключати 2G на своїх смартфонах. Однак онлайн-шахрайство виходить на новий рівень, при якому зростає кількість афер із використанням штучного інтелекту (ШІ) та QR-кодів. Так, у 2024 р. понад 83 % усіх шахрайських операцій в Україні відбулося в Інтернеті, а середня сума однієї незаконної операції зросла на 51 % – до 4761 грн. Такі дані наводить Ганна Довгальська, заступниця голови правління «Глобус Банку». Серед усіх найпоширеніших шахрайських схем експерти виділяють три особливо небезпечні: цифровий скімінг (при покупці в онлайн-магазині користувач вводить дані картки* *на нібито звичайному сайті, але через прихований шкідливий код їх миттєво перехоплюють шахраї); квішинг (шкідливі QR-коди, які ведуть на фейкові сайти, їх розміщують у громадських місцях, на афішах, банкоматах або надсилають у месенджерах); шахрайство зі штучним інтелектом (завдяки штучному інтелекту шахраї створюють надпереконливі фальшиві голоси, електронні листи й навіть чат-боти). Зауважено, що навіть найкраща кіберсистема не врятує, якщо користувач не дотримується базових правил безпеки.* Текст: <https://fakty.ua/456887-top-3-shemy-kibermoshennichestva-v-ukraine-kak-obmanyvayut-i-est-li-sposoby-zacshity>
17. **Ткаченко В. В. Гібридні форми тероризму: кримінологічний аспект** [Електронний ресурс] / Валентина Василівна Ткаченко // Право.UA: наук.-практ. журн.– 2025. – № 2. – С. 93-99. *Досліджено феномен гібридного тероризму, який є важливою складовою сучасних гібридних воєн, що поєднують традиційні методи ведення бойових дій із новітніми техніками, такими як інформаційні кампанії, кібернетичні атаки, економічний тиск і терористичні акти. Вказано, що гібридний тероризм спрямований на дестабілізацію державних інститутів, підрив політичних та економічних систем, а також на ослаблення морального духу населення. Окреслено основні форми гібридного тероризму, розкрито суть інформаційного тероризму, який включає медіатероризм і кібертероризм. Наголошено на важливості розуміння психологічних і соціальних факторів, що сприяють радикалізації осіб, які приєднуються до терористичних угруповань, серед яких – соціальна нерівність, політична нестабільність і глобалізація інформаційних технологій.* Текст: <https://pravo.unesco-socio.in.ua/wp-content/uploads/archive/Pravo-ua-2025-2/Pravo_ua_2025_2_093.pdf>
18. **Шевченко Ю. Масована кібератака на Францію: хакери викрали інформацію про підводні човни і ядерну зброю** [Електронний ресурс] / Юлія Шевченко // Focus.ua : [вебсайт]. – 2025. – 29 лип. – Електрон. дані. *Як повідомило видання «The Financial Times», французька оборонна компанія «Naval Group» стала жертвою кібератаки. Внаслідок цього хакери отримали доступ до конфіденційних даних про підводні човни та фрегати. Вказано, що хакери виклали 30 ГБ даних «Naval Group» – суднобудівної компанії, яка виробляє французькі підводні човни та фрегати, зловмисник обіцяє викласти ще більше документів. У витоку міститься, зокрема, початковий код бойових систем, програмне забезпечення ядерної зброї підводних човнів, внутрішні електронні листи, посібники, мережеві дані. Наразі «Naval Group» проводить розслідування й аналізує справжність опублікованих документів. Зазначено, що окрім постачання французькому флоту, компанія має контракти з флотами та урядами різних країн світу на постачання підводних човнів, кораблів та оборонних систем*. Текст: <https://focus.ua/uk/voennye-novosti/716796-masovana-kiberataka-na-franciyu-hakeri-otrimali-dostup-do-informaciji-pro-pidvodni-chovni-i-yadernu-zbroyu>
19. **Як посилити демократичну стійкість у добу гібридних атак?** [Електронний ресурс] / Прес-служба Апарату Верхов. Ради України // Голос України. – 2025. – 18 лип. (№ 392). – Електрон. дані.*Подано інформацію, що заступник голови Комітету Верховної Ради України (ВР України) з питань правоохоронної діяльності Галина Михайлюк взяла участь у 107-му семінарі Rose-Roth (формат міжпарламентського діалогу, організований Парламентською асамблеєю НАТО спільно з Європарламентом для обговорення питань підтримання безпеки та демократії), який відбувся у Брюсселі. Зауважено, що у центрі уваги учасників семінару – стратегічна співпраця ЄС і НАТО як фундамент політичної стійкості та ключовий елемент захисту наших цінностей, інституцій і демократичного способу життя. Панельні дискусії охопили широкий спектр викликів: від зовнішнього втручання у вибори, кампаній з дезінформації і кіберзагроз – до ролі парламентського контролю в секторі безпеки та зміцнення інституційної спроможності.* Текст: <https://www.golos.com.ua/article/385268>

**Підготовлено відділом інформаційного забезпечення органів влади**

**Національної бібліотеки України імені Ярослава Мудрого**

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

**31.07.2025**