**Кібербезпека**

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

***анотований бібліографічний список***

***2025. – Вип. 9 (вересень). – 8 с.***

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

1. **Актуальні питання розвитку юридичної науки в період воєнного стану** : міжнар. наук.-практ. конф., 17 трав. 2024 р., [Львів]. – Львів ; Торунь : Liha-Pres, 2024. – 165 с. : табл. ***Шифр зберігання в Бібліотеці: А838564*** *Зі змісту:**Протидія кібератакам в період російсько-української війни / О. М. Марчук, Д. О. Богатько. – С. 90-93.*
2. **Актуальні проблеми протидії корупції в умовах воєнного стану** :міжнар. наук.-практ. конф., 15 лют. 2024 р., [Львів]. – Львів ; Торунь : Liha-Pres, 2024. – 155 с. ***Шифр зберігання в Бібліотеці: А838563*** *Зі змісту:* *Боротьба з кіберзлочинністю в умовах війни в Україні / Б. М. Білецький, С. В. Клюйко. – С. 14-17.*Текст: <https://sipl.com.ua/wp-content/uploads/2024/04/conf_SIPL_law_%D0%BB%D1%8E%D1%82%D0%B8%D0%B9.pdf>
3. **Арпентій С. П.** **Стратегічні засади забезпечення кібербезпеки США** [Електронний ресурс] / С. П. Арпентій // Інформація і право. – 2025. – № 2 (53). – С. 176-182. *Проаналізовано* розвиток і формування стратегічних засад забезпечення кібербезпеки США. Висвітлено основні пріоритети національних стратегій забезпечення кібербезпеки. Вказано, що еволюція формування стратегій забезпечення кібербезпеки США свідчить про застосування нового комплексного підходу, зміст якого полягає в інтегрованому стримуванні  агресії у кіберпросторі. Проаналізовано нову Стратегію кібербезпеки США 2023 року, положення якої  передбачають покращання співпраці між федеральним урядом і приватним сектором, а також поліпшення стандартів виправлення вразливостей у комп’ютерних системах. Констатовано, що складність зростаючих кіберзагроз, які посилені розвитком штучного інтелекту (ШІ), спонукають федеральні органи США вживати більш дієвих заходів захисту комп’ютерних систем. Акцентовано, що посилення кіберзагроз змушує федеральний уряд США збільшувати бюджет на кібербезпеку, стимулювати інвестиції в дослідження ШІ для ефективного запобігання кібератакам. Текст: <http://il.ippi.org.ua/article/view/334229>
4. **Возник М. В. Теоретико-правові основи протидії тероризму** [Електронний ресурс] / Михайло Володимирович Возник, Юрій Віталійович Будяк // Нац. інтереси України. – 2025. – № 9. – С. 542-551. *Проаналізовано теоретико-правові основи протидії тероризму в умовах сучасних глобальних викликів і гібридних загроз національній безпеці. Досліджено еволюцію доктринальних підходів до визначення тероризму від класичних концепцій до сучасних інтерпретацій, що враховують кібертероризм, біотероризм та інформаційний тероризм. Висвітлено систему міжнародно-правового регулювання антитерористичної діяльності, включаючи конвенції Організації Об’єднаних Націй (ООН), рішення Ради Безпеки, директиви Європейського Союзу (ЄС) та двосторонні угоди про співробітництво у сфері боротьби з тероризмом. Розглянуто національні правові механізми протидії тероризму, систему суб’єктів антитерористичної діяльності (правоохоронні органи, спеціальні служби, військові формування) та принципи їх координації в межах єдиної системи забезпечення національної безпеки. Особливу увагу приділено проблемам забезпечення балансу між вимогами національної безпеки та дотриманням фундаментальних прав людини, зокрема права на приватність, свободу пересування та справедливий суд. Визначено сучасні виклики правового регулювання антитерористичної діяльності: транснаціональний характер терористичних загроз, використання новітніх технологій терористами, складності міжнародного співробітництва. Запропоновано концептуальні підходи до вирішення виявлених проблем, включаючи удосконалення міжнародної правової бази, розвиток превентивних механізмів, посилення інформаційної безпеки та підвищення ефективності міжвідомчої координації.* Текст: <http://perspectives.pp.ua/index.php/niu/article/view/28694/28652>
5. **Демедюк С. В. Темна сторона комп’ютерних мереж: злочини та незаконна діяльність онлайн** [Електронний ресурс] / С. В. Демедюк // Прав. новели. – 2025. – № 26. – С. 157-165. *Досліджено основні аспекти нелегальної діяльності в комп’ютерних мережах, проаналізовано її соціальні, економічні та технологічні чинники. З'ясовано, що основними видами злочинів є несанкціоноване втручання в роботу інформаційних систем, використання даних і розповсюдження шкідливого програмного забезпечення. Висвітлено співвідношення поширення цієї групи злочинів за рівнем ризику на основі експертної думки та статистичних даних Єдиного реєстру досудових розслідувань (ЄРДР). Окреслено відповідні статті Кримінального кодексу України (КК України) та окрему увагу приділено проблемам кіберзлочинності в Україні, особливо в контексті гібридної війни та атак на критичну інфраструктуру. Представлено статистичний аналіз злочинних методів, використаного програмного забезпечення та каналів поширення незаконної діяльності, що дозволяє виокремити ключові тенденції. Акцентовано на необхідності адаптації законодавства до нових викликів, посилення міжнародної співпраці та вдосконалення механізмів моніторингу.* Текст: <http://legalnovels.in.ua/journal/26_2025/20.pdf>
6. **Довгань О. Д. Протидія counter-forensics як складова цифрової безпеки критичної інфраструктури України** [Електронний ресурс] / О. Д. Довгань, Т. Ю. Ткачук // Інформація і право. – 2025. – № 2 (53). – С. 115-125. Досліджено контрфорензіку як одну з найбільш небезпечних форм цифрового втручання, що є прямою загрозою цифровій безпеці об’єктів критичної інфраструктури України в умовах повномасштабної війни. Обґрунтовано, що контрфорензічні технології – зокрема wiping, fileless-атаки, стеганографія, діпфейки та інші інструменти приховування цифрових слідів – активно використовуються у сучасних кібератаках, спрямованих на підрив стійкості ключових елементів інфраструктури держави. Здійснено міждисциплінарний аналіз технічних, правових і організаційних аспектів протидії контрфорензіці. Розглянуто реальні кейси втручань у роботу енергетичних, логістичних, телекомунікаційних та адміністративних систем, під час яких зловмисники здійснювали спроби приховати або знищити цифрові докази. Особливу увагу приділено національному та міжнародному досвіду захисту цифрових слідів, зокрема методам резервного збереження журналів, використанню засобів аналітики на основі штучного інтелекту, інституційним моделям співпраці між державними та приватними структурами. Надано пропозиції щодо удосконалення нормативно-правового регулювання електронних доказів для об’єктів критичної інфраструктури, а також рекомендації з технічного переоснащення судово-експертної та оперативної інфраструктури. Обґрунтовано доцільність створення Національного архіву цифрових доказів та запровадження обов’язкової сертифікації фахівців із цифрової криміналістики з урахуванням компоненту контрфорензіки. Текст: <http://il.ippi.org.ua/article/view/334135>
7. **Дронова А. «Кібербезпека – спільна справа»: у Києві на IT Meets обговорили, як бізнесу захистити дані й репутацію** [Електронний ресурс] / Аліна Дронова // Fakty.ua : [вебсайт]. – 2025. – 3 верес. – Електрон. дані. *Йдеться про зустріч «Кібербезпека: як бізнесу захиститися від загроз», на якій учасники від IT Meets ділилися досвідом, дискутували та пропонували практичні рішення, які допомагають компаніям залишатися стійкими в епоху цифрових ризиків. Обговорено, хто у 2025 р. реально відповідає за безпеку в компанії, чому формальна сертифікація не гарантує захисту та як правильно говорити з клієнтами у випадку кіберінциденту. Виступи стосувалися і стандартів ISO/IEC 27001, і перевірок контрагентів через KYC/KYS, і нових вимог міжнародних партнерів. Експерти звернули увагу на відмінності між інформаційною та ІТ-безпекою, окреслили виклики у збереженні даних і довіри клієнтів, а також наголосили на важливості вибору дієвої моделі управління ризиками, яка охоплює всі процеси компанії*. Текст: <https://fakty.ua/459400-kiberbezopasnost-obcshee-delo-v-kieve-na-it-meets-obsudili-kak-biznesu-zacshitit-dannye-i-reputaciyu>
8. **Жеребець** **О. М. Правове забезпечення методики ідентифікації та оцінки кіберризиків на національному рівні: сучасний досвід Словаччини та Латвії** [Електронний ресурс] / О. М. Жеребець // Інформація і право. – 2025. – № 2 (53). – С. 164-175. Визначено поняття, зміст і складові оцінювання ризиків кібербезпеки, узагальнено фактори, які доцільно враховувати під час його проведення. Окреслено сучасні тенденції поширення кіберзагроз і кібератак. Деталізовано складові компоненти, визначено класифікацію, види, мету та завдання оцінювання кіберризиків та елементи методики її здійснення. Акцентовано увагу на ініціативах України в контексті розробки та реалізації планових заходів у сфері посилення кібербезпеки держави в умовах правового режиму воєнного стану. Розглянуто позитивний досвід Словаччини та Латвії з нормативного забезпечення стратегічних засад кібербезпеки, методики ідентифікації та оцінювання кіберризиків на національному рівні. Визначено роль та значення оцінки кіберризиків для єдиної інформаційної системи кібербезпеки цих країн. Окреслено подальші напрямки удосконалення національної системи забезпечення кібербезпеки в контексті необхідності прискорення розроблення та затвердження методики ідентифікації та оцінки кіберризиків на національному рівні, нормативного врегулювання питань щодо впровадження обов’язковості проведення їх оцінювання. Текст: <http://il.ippi.org.ua/article/view/334163>
9. **Краснолуцька О. Миротворці і ракети. Гарантії безпеки від Європи** [Електронний ресурс] / Олеся Краснолуцька // Korrespondent.net : [вебсайт]. – 2025. – 4 верес. – Електрон. дані. *Окреслено підсумки зустрічі у Парижі 35 лідерів із Коаліції охочих, на якій союзники України завершили узгодження гарантій безпеки та звернулися до Президента США Дональда Трампа за підтримкою, аби такі гарантії стали реальністю. Як зазначив Президент Франції Еммануель Макрон, 26 країн готові взяти участь у міжнародних силах як частині гарантій безпеки для України у разі мирної угоди з РФ; жодних обмежень чисельності армії України та відновлення армії; найближчими тижнями буде визначено роль США у цих процесах тощо. Польський прем’єр Дональд Туск підтвердив, що деякі держави гарантують свою присутність, або участь у механізмах безпеки України, але Польща не передбачає направлення солдатів на українську територію. Італія теж готова підтримати потенційне припинення вогню шляхом ініціатив із моніторингу та навчання за межами України, але не планує направляти війська в країну, про що зауважила прем’єрка Джорджа Мелоні. Офіс прем’єр-міністра Великої Британії Кіра Стармера повідомив, що «коаліція охочих» оголосила про постачання Україні далекобійних ракет для подальшого зміцнення її арсеналу. Коментуючи зустріч, Президент України Володимир Зеленський відзначив готовність кожної з країн зробити внесок у гарантування безпеки на землі, морі, у повітрі та кіберпросторі. Після саміту у Парижі український лідер провів телефону розмову з Президентом США Д. Трампом і запропонував Вашингтону розглянути спеціальний формат для захисту українського неба.* Текст: <https://ua.korrespondent.net/ukraine/4813219-myrotvortsi-i-rakety-harantii-bezpeky-vid-yevropy>
10. **Лесько Н. В. Перешкоди до дотримання принципу доброчесності суддів в умовах воєнного стану** [Електронний ресурс] / Наталія Володимирівна Лесько // Нац. інтереси України. – 2025. – № 9. – С. 585-596. *Окреслено ключові перешкоди дотримання принципу доброчесності суддів в умовах воєнного стану з урахуванням наслідків пандемії COVID–19. Схарактеризовано інституційні, процесуальні, етичні та технологічні чинники ризику. Встановлено, що накладання дистанційних практик, успадкованих від пандемії, на реалії повномасштабного збройного вторгнення підсилює кіберризики, ускладнює ідентифікацію учасників процесу, перевірку достовірності доказів і збереження таємниці нарадчої кімнати. Доведено, що окремі процедурні спрощення без належних запобіжників призводять до асиметрій у змагальності сторін і підривають суспільну довіру до мотивів рішень. Запропоновано шляхи вирішення означених проблем, серед яких: прозорі протоколи роботи з матеріалами з обмеженим доступом; автоматизований і публічний розподіл справ із неможливістю ручного втручання; захист викривачів тощо.*  Текст: <http://perspectives.pp.ua/index.php/niu/article/view/28698/28656>
11. **Лісовський П. М. Міжнародно-правове регулювання штучного інтелекту в сучасному кіберкапіталі** / П. М. Лісовський, Ю. П. Лісовська. – Київ : Ліра-К, 2025. – 175 с. ***Шифр зберігання в Бібліотеці: А839953*** *У монографії розкрито міжнародно-правове поле регулювання ШІ, що є**нормативно-ціннісним пріоритетом як фундаментальний вектор розвитку сучасного кіберкапіталу.**Зосереджено увагу на феноменально-екзистенційних підходах цифрового безсмертя щодо креативної особи. Концептуально здійснено міжнародно-правову перевірку щодо ефективності математичної моделі ШІ, в якому сучасне кіберкапітальне забезпечення, зокрема нафтогазових об’єктів підвищеного ризику як критичної інфраструктури, відіграє пріоритетно-стратегічну роль у державі та суспільстві. Прогнозовано міжнародно-правовий механізм захисту навігаційної структури ШІ як кластерного аерокосмічного комплексу в системі кіберкапіталу.*
12. **Мануілов Я. С.** **Європейський досвід забезпечення кібербезпеки** [Електронний ресурс] / Я. С. Мануілов // Інформація і право. – 2025. – № 2 (53). – С. 147-154. Проаналізовано ключові тенденції і події, які визначають політику ЄС у сфері забезпечення кібербезпеки. Розглянуто основні нормативні акти ЄС у цій сфері. Звернено увагу на європейський досвід застосування режиму «кіберсанкцій». Висвітлено нові стандарти кібербезпеки, які є обов’язковими до виконання на всій території ЄС. Підкреслено, що застосування найсучасніших технологій штучного інтелекту (ШІ) може кардинально поліпшити роботу команд з кібербезпеки, підвищуючи їх ефективність і зменшуючи існуючі кіберризики. Зроблено висновок, що для досягнення стратегічних цілей у сфері кібербезпеки Україна має посилити спроможності у протидії кіберзлочинності шляхом проведення спільних з ЄС заходів, спрямованих на підвищення стійкості в кіберпросторі. Текст: <http://il.ippi.org.ua/article/view/334153>
13. **Матеріали Всеукраїнської науково-практичної конференції «Актуальні проблеми кримінального права і процесу та шляхи їх вирішення»**: присвяч. наук. шк. д-ра юрид. наук, проф., проф. Каф. кримін. права та процесу Нікітіна Юрія Вікторовича з нагоди його 70-річчя : [Ірпінь, 12 груд. 2024 р.] / [уклад. Н. А. Сперкач ; за заг. ред. Г. В. Дідківської]. – Вінниця : Нілан-ЛТД, 2025. – 223 с. – ***Шифр зберігання в Бібліотеці : А839364****Зі змісту: Заходи запобігання кіберзлочинності в кримінологічній теорії: сучасний стан та напрями вдосконалення / Н. А. Сперкач, М. О. Сперкач. – С. 12-19; Кіберзлочини у сучасному світі: методи розслідування та виклики / А. Р. Єроменко. – С. 107-110; Відповідальність за правопорушення у сфері кіберзахисту персональних даних: кейси світових цифрових гігантів і виклики для України / М. Г. Максіменцев. – С. 195-200; Зарубіжний досвід у протидії розвитку кібершахрайства / Г. М. Воробей. – С. 200-204; Протидія кіберзлочинності в умовах воєнного стану / К. І. Король. – С. 208-211.*
14. **Федорченко О. С.** **Проблеми імплементації додаткового протоколу до конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп’ютерні системи** [Електронний ресурс] / О. С. Федорченко // Інформація і право. – 2025. – № 2 (53). – С. 183-192. Проаналізовано міжнародні акти з питань боротьби із нетерпимістю, мовою ненависті та іншими злочинами на ґрунті ненависті, а також нормативно-правову базу України у сфері протидії злочинам на ґрунті ненависті та дискримінації. Розглянуто проблеми застосування норм, що встановлюють відповідальність за порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками. Досліджено досвід окремих зарубіжних країн у частині імплементації Додаткового протоколу до конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобського характеру, вчинених через комп’ютерні системи. Надано рекомендації щодо імплементації в національне законодавство цього Додаткового протоколу. Текст: <http://il.ippi.org.ua/article/view/334230>

**Підготовлено відділом інформаційного забезпечення органів влади**

**Національної бібліотеки України імені Ярослава Мудрого**

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

**30.09.2025**