Кібербезпека

(інформаційні злочини, інформаційний тероризм):

анотований бібліографічний список

2025. – Вип. 12 (грудень). – 5 с.

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

1. **Білецький В. О. Правово-теоретичні засади функціонування Державної прикордонної служби України в умовах сучасного безпекового середовища** [Електронний ресурс] / Вячеслав Олександрович Білецький, Володимир Миколайович Матняк // Наук. перспективи. – 2025. – № 11. – С. 1095-1106. *Розкрито правові та теоретичні основи функціонування Державної прикордонної служби України (ДПСУ) в умовах воєнного стану та активних трансформацій правового поля. Розкрито зміст основних напрямів розвитку правового регулювання у сфері оперативно-розшукової діяльності, охорони кордону, інформаційної безпеки та міжнародного співробітництва. Окрему увагу приділено впровадженню цифрових технологій, технічних систем спостереження, безпілотних літальних апаратів (БПЛА), аналітичних платформ і засобів штучного інтелекту (ШІ) для підвищення ефективності контролю та мінімізації впливу людського фактора. Проаналізовано законодавчі зміни 2023 – 2025 рр., які стосуються модернізації правового статусу прикордонників, посилення антикорупційних механізмів, розбудови системи кіберзахисту та вдосконалення координації між суб'єктами сектора безпеки. Зроблено висновок, що підвищення ефективності функціонування ДПСУ можливе лише за умови системного оновлення правових і теоретичних засад її діяльності, розвитку міжвідомчої взаємодії, формування нової концепції управління прикордонною безпекою та інтеграції сучасних технологічних рішень у практику охорони державного кордону*. Текст: https://perspectives.pp.ua/index.php/np/article/view/32668/32625

2. **Залата О. Невидимий фронт: як хакери б'ються на війні в Україні та коли ШІ стане новою зброєю** [Електронний ресурс] / Олександр

Залата // Focus.ua : [вебсайт]. – 2025. – 24 груд. – Електрон. дані. *Йдеться про те, що в епоху глобальної цифровізації та ШІ з'явилася «кіберзброя», яка безпосередньо впливає на перебіг війни в Україні: військові хакери виводять з ладу критично важливі системи, зривають постачання зброї та живої сили, видобувають цінні розвіддані, які дають змогу проводити контрнаступи, знищувати більше окупантів і рятувати життя. Розглянуто, що таке «кіберзброя», розкрито роль ШІ у кіберзахисті. Фахівець із кібербезпеки Є. Поремчук розповів, як насправді використовується кіберзброя на війні в Україні, чи робить ШІ її ще небезпечнішою, а також розкрив ефективність кібератак і навів кілька гіпотетичних прикладів, як вони впливають на бойові дії.* Текст: https://focus.ua/uk/digital/737177-kiberzbroya-na-viyni-v-ukrajini-yak-shkodit-ai-posilyuye-kiberataki

3. **Краснолуцька О. Термін до 2027 року. США виходять з НАТО?** [Електронний ресурс] / Олеся Краснолуцька // Korrespondent.net : [вебсайт]. – 2025. – 10 груд. – Електрон. дані. *Вказано, що соратник Д. Трампа республіканець Т. Массі вніс законопроєкт про вихід США з НАТО та перенаправлення мільярдів доларів на власну оборону. Агентство «Reuters» повідомило, що минулого тижня у Вашингтоні на зустрічі співробітників Пентагону та європейських делегацій не було озвучено планів щодо виходу з Альянсу. Проте Вашингтон висунув вимогу, щоб Європа до 2027 р. взяла на себе більшість конвенційних оборонних можливостей НАТО – від розвідки до ракет. Американські чиновники повідомили своїм колегам, що якщо Європа не виконає вимоги до 2027 р., США можуть припинити участь у деяких механізмах координації оборони НАТО. Як заявили кілька європейських чиновників, термін 2027 р. не є реалістичним, незалежно від того, як Вашингтон оцінить прогрес. Європейський Союз (ЄС) поставив собі за мету підготувати континент до самозахисту до 2030 р., оскільки має заповнити прогалини у своїй протиповітряній обороні (ППО), безпілотниках, можливостях кібервійни, боєприпасах тощо.* Текст: https://ua.korrespondent.net/world/4839325-termin-do-2027-roku-ssha-vykhodiat-z-nato

4. **Кривенко О. І. Оперативно-розшукова протидія шахрайствам, що вчиняються з використанням мережі Інтернет** / О. І. Кривенко, М. В. Стащак, В. В. Капустник ; НДІ публіч. права. – Харків : Панов А. М., 2025. – 207 с. : табл. ***Шифр зберігання в Бібліотеці: А841965*** *У монографії вперше подано авторське бачення перспективних напрямів впровадження зарубіжного досвіду з питання оперативно-розшукової протидії шахрайствам, що вчиняються з використанням мережі Інтернет. Вперше сформульовано авторські пропозиції і рекомендації щодо удосконалення правового регулювання оперативно-розшукової протидії таким шахрайствам. Результатом проведеного дослідження стало удосконалення оперативно-розшукової характеристики шахрайств, що вчиняються з використанням мережі Інтернет, і теоретично-практичних розробок щодо перспективних шляхів оптимізації організації оперативно-розшукової протидії таким шахрайствам.*

5. **Лиса А. Гібридна війна Росії випробовує Європу – FT** [Електронний ресурс] / Анна Лиса // Korrespondent.net : [вебсайт]. – 2025. – 9 груд. – Електрон. дані. *Наведено інформацію видання «Financial Times» із посиланням на європейські спецслужби про низку диверсій РФ у Європі, що може бути частиною масштабної підготовки до війни та формує картину стратегічної ескалації. Останні дії РФ розглядаються у контексті доповіді НАТО «Спільна оцінка загроз» від 2023 р., де вказано, що до 2029 р. РФ може підготувати свої збройні сили та економіку до війни з Європою. Згадано низку розкритих операцій у Польщі, Німеччині, Великій Британії, Литві. Вказано, що представники європейських спецслужб стежать за російськими агентами, які здійснюють диверсії; РФ використовує також місцевих і східноєвропейських громадян, включно з українцями, яких наймають через месенджери. Зауважено, що велика кількість гібридних атак та їх аналіз дозволяють спецслужбам побачити закономірності та встановити зв'язки між подіями навіть тоді, коли участь РФ не була доведена чи виявлена. Фахівці наголошують, що нинішня активність РФ в Європі відповідає середній «передвоєнній» фазі, схожій на плани КДБ у радянські часи: у мирні часи атаки менш масштабні та маскуються під нещасні випадки, а у разі війни*

активізується ціла мережа агентів для проведення деструктивних дій. Текст: https://ua.korrespondent.net/world/4838960-hibrydna-viina-rosii-vyprobovuie-yevropu-FT

6. **Плетньов О. В. Цифрові докази у протидії дезінформації та діпфейкам щодо воєнних злочинів** [Електронний ресурс] / О. В. Плетньов, Є. В Коваленко // Юрид. наук. електрон. журн. – 2025. – № 10. – С. 265-268. *Йдеться про цифрові докази у протидії дезінформації та діпфейкам щодо воєнних злочинів. Висвітлено процес використання генеративного штучного інтелекту (ШІ) для створення діпфейків в інформаційних операціях проти України та вказано, що текст, згенерований ШІ, залишається проблемою для розвідки, оскільки загальнодоступні інструменти не можуть надійно виявляти його, особливо в текстах невеликого обсягу, таких як коментарі в соціальних мережах. Запропоновано застосування двох підходів для боротьби з діпфейками: технічне виявлення та стратегія реагування, яка охоплює загальну обізнаність з проблемою, постійний рівень залучення до вирішення проблеми діпфейків у поєднанні з моніторингом засобів масової інформації (ЗМІ) та здатністю швидко виявляти та оцінювати потенційні фальсифікації з технічної точки зору.* Текст: http://lsej.org.ua/10_2025/61.pdf

7. **Роль архівних установ у забезпеченні інформаційної безпеки** [Електронний ресурс] / Ігор Саламаха, Ірина Денис, Валентина Новосад, Любов Шептицька // Вісн. Кн. палати. – 2025. – № 10. – С. 27-33. *Розглянуто актуальну проблему забезпечення інформаційної безпеки в діяльності архівних установ в умовах цифрової трансформації та гібридних загроз. Проаналізовано наукові підходи до трактування інформаційної безпеки у сфері архівознавства, схарактеризовано основні функції архівних установ зі збереження, захисту й автентифікації інформаційних ресурсів. Визначено основні загрози цифровим архівам, серед яких: кібератаки, фальсифікація документів, технічні проблеми, інсайдерські ризики та недосконалість правового регулювання. Увагу приділено перспективним напрямам інтеграції архівної сфери в національну систему інформаційної безпеки. Запропоновано комплекс заходів нормативного, організаційного, технологічного й освітнього*

характеру, реалізація яких сприятиме підвищенню стійкості держави до інформаційних загроз, збереженню історичної пам'яті та формуванню довіри до верифікованої інформації. Текст: http://visnyk.ukrbook.net/article/view/343787

Підготовлено відділом інформаційного забезпечення органів влади Національної бібліотеки України імені Ярослава Мудрого
Відповідальний за випуск: Зайченко Н. Я.
29.12.2025