**Інформаційна безпека:**

***анотований бібліографічний список***

***2025. – Вип. 5 (травень). – 15 с.***

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

1. **Авраменко М. В. Методи протидії інформаційним бульбашкам в соціальних мережах: практичний аспект забезпечення інформаційної стійкості** [Електронний ресурс] / М. В. Авраменко, Д. О. Авраменко // Вісн. Нац. ун-ту оборони України : зб. наук. пр. – 2025. – № 3 (85). – С. 7-15. *Вказано, що в умовах сучасного інформаційного протистояння особливої актуальності набуває розробка та впровадження практичних методів протидії формуванню інформаційних бульбашок у соціальних мережах. Дослідження сфокусовано на конкретних інструментах і методиках, які можуть бути застосовані для підвищення інформаційної стійкості суспільства. Проаналізовано ефективність різних підходів до руйнування алгоритмічної ізоляції користувачів та забезпечення різноманітності інформаційного поля. Результати дослідження мають безпосереднє практичне значення для фахівців у сфері інформаційної безпеки, медіа-експертів і розробників політик протидії дезінформації.*  Текст: <http://visnyk.nuou.org.ua/article/view/322407/316534>
2. **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>
3. **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>
4. **Буняк В. У ЄС почала діяти нова система захисту прав користувачів у соціальних мережах** [Електронний ресурс] / Валерія Буняк // Детектор медіа : [інтернет-вид.]. – 2025. – 13 трав. – Електрон. дані. *Подано інформацію, що сім європейських компаній офіційно запустили Європейську мережу органів позасудового вирішення спорів відповідно до Закону про цифрові послуги (DSA), щоб допомогти користувачам захищати свої права в Інтернеті. До нової мережі долучилися німецька компанія «User Rights», сертифікована Федеральним агентством мереж, ірландський «Appeals Center Europe» (ACE), який з листопада приймає звернення щодо видалення або збереження контенту на фейсбуку, тіктоку та ютубі, «Adroit» (Мальта), «Central European Appeals Hub» (Словаччина), «Impress Dispute Resolutions» (Ірландія), «MFSD» (Італія) та «Vitarendező Tanács» (Угорщина). Їхньою метою є налагодження обміну досвідом, спрощення комунікації між платформами, користувачами та регуляторами, забезпечення незалежного перегляду рішень соцмереж щодо контенту.* Текст: <https://ms.detector.media/internet/post/37930/2025-05-13-u-ies-pochala-diyaty-nova-systema-zakhystu-prav-korystuvachiv-u-sotsialnykh-merezhakh/>
5. **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>
6. **Варналій К. Обмеження свободи вираження в кримінальному процесі: коли пост у Facebook стає доказом** [Електронний ресурс] / Катерина Варналій // Юрид. практика. – 2025. – 19 трав. – Електрон. дані. *Розглянуто питання притягнення до кримінальної відповідальності за дописи у Facebook та інших соціальних мережах, які можуть розцінюватися як публічні висловлювання з відповідними правовими наслідками. Окреслено статті Кримінального кодексу України (КК України) щодо кримінальної відповідальності за поширення інформації в Інтернеті та зазначено, що Кримінальним процесуальним кодексом України (КПК України) закріплено, які документи можуть бути визнані допустимими та використаними як доказ, якщо вони були належним чином зафіксовані. Проаналізовано судову практику з означеного питання та наголошено, що Конституцією України кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, що також закріплено у ст. 10 Європейської конвенції з прав людини, але національне і міжнародне законодавство визнає, що це право не є абсолютним та може бути обмежене в інтересах національної безпеки та громадського порядку.* Текст: <https://pravo.ua/obmezhennia-svobody-vyrazhennia-u-kryminalnomu-protsesi-koly-post-u-facebook-staie-dokazom/>
7. **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>
8. **Захист національної безпеки: хто і за яких умов може набувати право власності на українські медіа** [Електронний ресурс] // Юрид. газ. – 2025. – 6 трав. – Електрон. дані. *Відповідно до Закону України «Про запобігання загрозам національній безпеці, пов'язаним із надмірним впливом осіб, які мають значну економічну та політичну вагу в суспільному житті (олігархів)», право власності на медіа обмежується для осіб, внесених до реєстру олігархів. Також відповідно до Закону України «Про медіа» заборонено набуття права власності громадянами держави-агресора, юридичними особами, пов'язаними з державою-агресором, а також особами, щодо яких застосовані санкції. Розглянуто такі питання: як перевіряється потенційний покупець медіа; на що звертається увага під час перевірки.* Текст: <https://yur-gazeta.com/golovna/zahist-nacionalnoyi-bezpeki-hto-i-za-yakih-umov-mozhe-nabuvati-pravo-vlasnosti-na-ukrayinski-media.html>
9. **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:**Забезпечення інформаційної безпеки під час війни / М. Шепітько. – С. 193-196; Стратегія інформаційної безпеки як інструмент публічно-управлінської діяльності / А. Розпаченюк. –   
   С. 354-357.*
10. **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/>
11. **Костенко Н. Від хаосу до регулювання: як змінюється правове поле для блогерів** [Електронний ресурс] / Назар Костенко // Юрид. газ. – 2025. – 21 трав. – Електрон. дані. *За словами автора статті, в епоху, коли соціальні мережі стали невіддільною частиною повсякденного життя, особливої ваги набули ті, хто формує в них тренди та впливає на аудиторію, – блогери. Україна, як і багато інших країн, прийшла до необхідності створення правового поля для регулювання їхньої діяльності, адже вплив блогерів на суспільну думку та споживчі звички аудиторії став надто вагомим, щоб залишатися поза законодавчим контролем. Розглянуто такі питання: законодавчі зміни та новий статус блогерів; обов'язкове маркування реклами та фінансова відповідальність; заборонений контент та етичні норми; блокування за незаконну рекламу: практика правозастосування; майбутнє регулювання: куди рухається законодавство? Наведено рекомендації для блогерів*. Текст: <https://yur-gazeta.com/dumka-eksperta/vid-haosu-do-regulyuvannya-yak-zminyuetsya-pravove-pole-dlya-blogeriv.html>
12. **Крок до більшої прозорості, відповідальності та співпраці між державними структурами, громадянським суспільством і медіаспільнотою** [Електронний ресурс] / Прес-служба Апарату Верхов. Ради України // Голос України. – 2025. – 14 трав. (№ 346). – Електрон. дані. *Подано інформацію, що відбувся круглий стіл на тему саморегуляції у сфері медіа, ключовою подією якого стало підписання меморандуму між Комітетом Верховної Ради України (ВР України) з питань свободи слова та Комісією з журналістської етики. Голова Комітету Ярослав Юрчишин наголосив, що саморегуляція – це процес, а не результат. У нинішніх умовах це не лише інструмент відповідальності, а й фактор національної єдності, довіри до медіа та державних інституцій. Вказано, що цей меморандум – не просто документ, а крок до більшої прозорості, відповідальності та співпраці між державними структурами, громадянським суспільством і медіаспільнотою. Метою угоди є спільне декларування цінностей, узгодження позицій і напрямів для координування зусиль, що сприятимуть розвитку професійної журналістики в Україні, підвищенню якості журналістського контенту, зменшенню фейків, маніпуляцій та розвитку України.* Текст: <https://www.golos.com.ua/article/383973>
13. **Кудрявський І. В. Стратегії нападу з активним застосуванням дій в інформаційному просторі** [Електронний ресурс] / І. В. Кудрявський // Право та держ. упр. : зб. наук. пр. – 2024. – Вип. 3. – С. 78-87. *Досліджено шляхи підвищення ефективності державного управління у сфері захисту інформаційного простору України в умовах інформаційно-психологічного впливу з боку противника. Проаналізовано історичний досвід і сучасні стратегії інформаційного нападу в контексті російсько-української війни. Використано комплекс наукових методів для оцінювання функціонування механізмів державного управління. Запропоновано організаційні заходи для посилення протидії деструктивному впливу в інформаційному просторі.* Текст: <http://www.pdu-journal.kpu.zp.ua/archive/3_2024/13.pdf>
14. **Кушнір І. П. Протидія дезінформації: організаційно-правовий аспект** [Електронний ресурс] / І. П. Кушнір, С. В. Адамчук // Аналіт.-порівнял. правознавство : електрон. наук. вид. – 2025.–№ 1. – С. 470-475. *Проаналізовано поняття дезінформації крізь призму правового регулювання, як соціальне явище у сучасному інформаційному суспільстві. Запропоновано розглядати дезінформацію як інформацію (дані) чи повідомлення, яке повністю чи частково є неправдивим, перекрученим, взятим із контексту з негативною метою (може бути будь-що: психологічний вплив, зміна поведінки та думок суб’єкта впливу, отримання даних про банківські картки, коди доступу/паролі, отримання грошей, дестабілізації у суспільстві, дискредитація органів влади, тощо). Сформульовано, що протидія дезінформації залежить від багатьох чинників, у тому числі від: нормативно-правових, інституційних, організаційних, освітніх, принципової позиції населення України щодо бажання оволодіти навичками її розпізнання та недопущення впливу, психологічної стійкості, інформаційної гігієни тощо.* Текст: <https://app-journal.in.ua/wp-content/uploads/2025/02/80.pdf>
15. **Лиса А. У списку Медведчук: ЄС запровадив санкції за гібридні атаки Росії** [Електронний ресурс] / А. Лиса // Korrespondent.net : [вебсайт]. – 2025. – 20 трав. – Електрон. дані. *Вказано, що Європейський Союз (ЄС) 20.05.2025 запровадив нові обмежувальні заходи проти 21 фізичної особи та шести організацій, причетних до дестабілізаційної діяльності РФ за кордоном. Уперше запроваджено секторальні санкції, котрі охоплюють активи, пов’язані з гібридними загрозами – судна, літаки, нерухомість, цифрову та комунікаційну інфраструктуру. Зазначено, що у відповідь на систематичну російську кампанію з медіа-маніпуляцій, ЄС отримав можливість призупиняти ліцензії російських ЗМІ, що перебувають під контролем Кремля, а також забороняти їм трансляцію на території ЄС. Водночас, згідно з Хартією основоположних прав ЄС, ці заходи не обмежують діяльність журналістів поза межами мовлення. У санкційному списку – колишній український політик і бізнесмен В. Медведчук, який контролював проросійські медіа та фінансував пропагандистський канал «Голос Європи» і проєкт «Інша Україна», представники російського ГРУ, причетні до підриву демократії в Естонії, та пропагандисти, які діяли в Німеччині.*  Текст: <https://ua.korrespondent.net/world/4783303-u-spysku-medvedchuk-yes-zaprovadyv-sanktsii-za-hibrydni-ataky-rosii>
16. **Ломачинська І. Виклики соціальних мереж у формуванні ціннісних орієнтирів українського інтернет-покоління** [Електронний ресурс] / Ірина Ломачинська, Оксана Рихліцька// Вісн. НЮУ ім. Ярослава Мудрого. Серія : Філософія, філософія права, політологія, соціологія : зб. наук пр.– Харків, 2025. – Т. 1 (№ 64). – С. 147-158. *Обґрунтовано, що соціальні мережі стали потужним інструментом впливу на суспільство, особливо на молодь. Лідери думок у мережах формують світогляд та поведінку, а штучний інтелект (ШІ) змінює способи комунікації. Зауважено, що у відповідь на ці виклики важливо розвивати критичне мислення та цифрову етику, щоб зменшити негативний вплив мереж на психічне здоров'я молоді.* Текст: <http://fil.nlu.edu.ua/article/view/324580>
17. **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>
18. **Складан А. А. Вплив фейків на формування соціального дискурсу в релігійних медіа** [Електронний ресурс] / Андрій Анатолійович Складан **//** Культур. альм. – 2025. – № 1. – С. 55-62. *Проаналізовано вплив сучасних медіа на суспільство та культуру, зокрема поширення фейкових новин у постінформаційному суспільстві. Акцентовано, що релігійний масмедійний простір увібрав у себе не найкращі риси політичних, заангажованих ЗМІ та соцмереж, де поширюють недостовірну інформацію, яка не підкріплена фактами й часто спотворена.* *Розглянуто роль технологій у маніпуляції свідомістю, формуванні публічної думки через «індустрію уваги» та «інформаційні бульбашки». Підкреслено загрози для громадської безпеки та важливість розробки засобів для виявлення недостовірної інформації. Акцент зроблено на необхідності захисту об’єктивного інформаційного простору як умови для стійкого суспільного розвитку.* Текст: <https://almanac.npu.kiev.ua/index.php/almanac/article/view/533/496>
19. **Стоян Т. А. Сучасна практика врегулювання регіональних конфліктів: безпековий та інформаційний виміри** [Електронний ресурс] / Т. А. Стоян, С. П. Дмитренко, О. С. Дмитренко // Гілея : зб. наук. пр. / Нац. ун-т ім. М. П. Драгоманова. – Київ, 2025. – Вип. 203/204 (№ 1/2). – С. 75-81. *Визначено чинники ескалації конфліктів, зокрема вплив інформаційної революції та маніпуляцій. Проаналізовано важливість інтеграції традиційної безпеки з новітніми інформаційними технологіями для ефективної стабілізації ситуації. Розглянуто роль штучного інтелекту (ШІ), медіаграмотності та міжнародної співпраці в забезпеченні інформаційної безпеки. Надано рекомендації щодо впровадження систем моніторингу, освітніх програм і міжнародної координації задля зміцнення регіональної та глобальної стабільності.* Текст: <http://gileya.org/index.php?ng=library&cont=long&id=291>
20. **Терзі О. О. Принципи забезпечення інформаційної безпеки держави: досвід України та зарубіжних країн** [Електронний ресурс] / О. О. Терзі // Право та держ. упр. : зб. наук. пр. – 2024. – Вип. 3. – С. 51-57. *Висвітлено принципи забезпечення інформаційної безпеки України як складника національної безпеки. Проаналізовано сучасні загрози, недоліки державної політики у цій сфері та наголошено на важливості інтеграції в глобальне інформаційне середовище. Визначено необхідність законодавчого закріплення принципів інформаційної безпеки та адаптації найкращих міжнародних практик. Окреслено ключові напрями розвитку, зокрема створення нормативної бази, взаємодію державних і приватних структур та підвищення інформаційної грамотності.* Текст: <http://www.pdu-journal.kpu.zp.ua/archive/3_2024/9.pdf>
21. **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.*
22. **У 2024 році кожна п’ята дитина готова була зустрітися з незнайомцем з інтернету, – дослідження** [Електронний ресурс] // Детектор медіа : [інтернет-вид.]. – 2025. – 7 трав. – Електрон. дані. *Повідомлено, що у Києві відбулася пресконференція на тему онлайн-безпеки дітей у воєнні часи за участі представників уряду, посольств, бізнесу та громадських організацій. Восени 2024 р. громадська організація ”Dignity Online by #stop\_sexтинг” за підтримки Державної служби якості освіти, Crown Agents Ukraine, спільно з Proinsight Lab провели всеукраїнське дослідження про досвід українських дітей в інтернеті у воєнні часи. Про це розповіли в організації ”Dignity Online”. Повідомлено, що в опитуванні взяло участь 1799 дітей віком 10 – 17 років з усієї України, окрім тимчасово окупованих територій (ТОТ) АР Крим та Донецької, Луганської, Херсонської і Запорізької областей. Мета – дослідити досвід сексуального насильства та сексуальної експлуатації в інтернеті в українських дітей. Основними темами стали: поширеність епізодів сексуального насилля та сексуальної експлуатації онлайн серед дітей в Україні, використання штучного інтелекту (ШІ) як нового ризику сексуального насильства та сексуальної експлуатації дітьми та проти дітей, вплив воєнного контенту на онлайн-досвід дітей. Також дослідження стосувалося питання впливу сімейних стосунків на онлайн-безпеку дітей, зокрема, рівень довіри між батьками й дітьми та готовність дітей ділитися тривожними ситуаціями, з якими вони стикаються в інтернеті.* Текст: <https://ms.detector.media/internet/post/37904/2025-05-07-u-2024-rotsi-kozhna-pyata-dytyna-gotova-bula-zustritysya-z-neznayomtsem-z-internetu-doslidzhennya/>
23. **Українська Інформаційна Безпека: філологічний складник** = Ukrainian Information Security: Philological Component / [І. Р. Жиленко та ін.] ; за заг. ред. проф. Володимира Садівничого ; М-во освіти і науки України, Сум. держ. ун-т. – Суми : Сум. держ. ун-т, 2024. – 178, [1] с. : іл. ***Шифр зберігання в Бібліотеці: А837295*** *У монографії проаналізовано проблеми дезінформування як складника російсько-українського війни; поєднання теорій змов у часи криз для демократичного суспільства; питання інформаційної безпеки як ключового маркеру художньо-публіцистичної спадщини письменників еміграції: специфіки художньої репрезентації ідей інформаційної безпеки в сучасній українській прозі; девальвації та двоїстості значення слів як ключових аспектів філологічної складової інформаційної безпеки тощо. Порушено проблеми соціальної стійкості до ворожих наративів і формування власного воєнного наративу.*
24. **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.*
25. **Філіп`єва Д. Як захиститися від дезінформації та маніпуляцій: шість простих кроків** [Електронний ресурс] / Дар`я Філіп`єва // Детектор медіа : [інтернет-вид.]. – 2025. – 27 трав. – Електрон. дані. *Зазначено, що повномасштабне вторгнення РФ продовжило та масштабувало інформаційну війну. Дезінформація та пропаганда стали зброєю, а суспільство опинилося в умовах інформаційного перевантаження, масового поширення фейків і маніпуляцій. Також агресія спрямована на підрив довіри до медіа та намагається деморалізувати людей, посіяти сумніви, поширити паніку і вплинути на здатність приймати зважені рішення. Тож основним інструментом протидії дезінформації залишається медіаграмотність — комплекс навичок і знань, які дозволяють аудиторії ефективно взаємодіяти з медіа, розуміти їхній вплив і критично оцінювати інформацію. Розпізнати дезінформацію, оманливу, неправдиву, викривлену або помилкову інформацію можна за допомогою декількох простих кроків: перевірити першоджерело інформації; перевірити новину в кількох джерелах; перевірити факти; звернути увагу на світлини, аудіо або відеоматеріали; не попастися на клікбейт; перевірити, чи новина — не жарт.* Текст: <https://ms.detector.media/mediaosvita/post/37991/2025-05-27-yak-zakhystytysya-vid-dezinformatsii-ta-manipulyatsiy-shist-prostykh-krokiv/>
26. **Шевчук М. О. До питання конституційних засад інформаційної безпеки держави** [Електронний ресурс] / М. О. Шевчук // Аналіт.-порівнял. правознавство : електрон. наук. вид. – 2025.–№ 1. – С. 563-568. *Висвітлено конституційні засади інформаційної безпеки держави, зокрема такі принципи, як політичний та ідеологічний плюралізм, пріоритет прав і свобод людини, верховенство права, своєчасність та доцільність заходів протидії загрозам інформаційної безпеки, а також державний і громадський контроль у цій сфері. Підкреслено важливість вдосконалення законодавчої бази України в сфері інформаційної безпеки, а також необхідність підвищення ефективності контролю за дотриманням інформаційних прав і свобод як з боку держави, так і з боку громадськості.* Текст: <https://app-journal.in.ua/wp-content/uploads/2025/02/96.pdf>
27. **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>
28. **Шевчук М. О.** **Правове регулювання механізму забезпечення інформаційної безпеки** [Електронний ресурс] / М. О. Шевчук // Право та держ. упр. : зб. наук. пр. – 2024. – Вип. 3. – С. 58-63. *Проаналізовано питання інформаційної безпеки як ключового чинника захищеності держави та її життєво важливих сфер від інформаційних загроз. Особливу увагу приділено загрозам у сфері підприємництва, зокрема незаконній діяльності, порушенням у роботі з даними та людським помилкам. Обґрунтовано потребу в комплексному підході до інформаційної безпеки, вдосконаленні законодавства та впровадженні превентивних заходів із залученням державних і міжнародних структур.* Текст: <http://www.pdu-journal.kpu.zp.ua/archive/3_2024/10.pdf>
29. **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>
30. **Ященко В. А. Інформаційна безпека України: гуманітарно-правовий зріз** / Володимир Арсентійович Ященко ; Держ. наук. установа «Ін-т інформації, безпеки і права НАПН України». – Київ ; Одеса : Фенікс, 2024. – 295 с. ***Шифр зберігання в Бібліотеці: А838172*** *У монографії в гуманітарно-соціальному сенсі розглянуто актуальні проблеми забезпечення інформаційної безпеки України в синтезі її основних складових: філософсько-правових, етико-психологічних, інформаційно-політичних. Висвітлено предмет і метод інформаційного права, його місце і роль в системі інформаційної безпеки. Надано класифікацію інформаційних загроз та розглянуто їх трансформацію в умовах широкомасштабної збройної та інформаційної агресії РФ проти України.*

**Підготовлено відділом інформаційного забезпечення органів влади**

**Національної бібліотеки України імені Ярослава Мудрого**

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

**31.05.2025**