**Інформаційна безпека:**

***анотований бібліографічний список***

***2025. – Вип. 7 (липень). – 6 с.***

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

1. **Байда М. Видозміна практик споживання медіа в Україні: від традиційних до цифрових** [Електронний ресурс] / Марина Байда // Укр. культура: минуле, сучас., шляхи розвитку : наук. зб. / Рівнен. держ. гуманітар. ун-т. – Рівне, 2025. – Вип. 50. – С. 329-335. *Представлено еволюцію практик споживання медіа в Україні, досліджуючи шлях від звичних державних ЗМІ до розмаїття цифрових. Розглянуто історичні, політичні та технологічні імпульси, які спричинили ці зміни, зокрема, розпад СРСР, становлення незалежної журналістики та швидке поширення Інтернету. Увагу приділено ролі соціальних мереж і застосунків у вирішальні моменти як-от Революція Гідності, анексія Криму та теперішня російсько-українська війна. Продемонстровано перспективи використання цифрових медіа та значні виклики, пов’язані з дезінформацією та пропагандистськими атаками. Акцентовано на важливості підвищення медіаграмотності та підтримці незалежних ЗМІ для гарантування інформаційної безпеки України. Аргументовано, що вік залишається ключовим фактором у формуванні медіа-вподобань: старша аудиторія покладається на традиційні формати, тоді як молодші користувачі тяжіють до інтерактивних цифрових платформ.* Текст: <https://zbirnyky.rshu.edu.ua/index.php/ucpmk/article/view/980/1883>
2. **Горбань Ю. Трансформація інформаційної культури під впливом технологічних інновацій** [Електронний ресурс] / Юрій Горбань, Оксана Олійник // Укр. культура: минуле, сучас., шляхи розвитку : наук. зб. / Рівнен. держ. гуманітар. ун-т. – Рівне, 2025. – Вип. 50. – С. 420-426. *Мета дослідження – виявити взаємовплив суспільства знань, інформаційної культури та технологічних інновацій. Визначено, що технології не лише надають інструменти, але й фундаментально змінюють практики створення, поширення та інтерпретації знань, посилюючи роль візуальної культури та алгоритмічних систем. Глобалізація інформаційного простору створює умови як для безпрецедентного доступу до інформації, так і поширення маніпуляцій, посилення цифрового розриву. Встановлено, що ефективна навігація в цьому середовищі потребує розвинених компетенцій – не лише базової інформаційної, але й критичної медіа- та візуальної грамотності для протидії дезінформації та розуміння медіаефектів.* Текст: <https://zbirnyky.rshu.edu.ua/index.php/ucpmk/article/view/995/1898>
3. **Денисова Д. Банківську таємницю скасують: що саме планують розкривати банки** [Електронний ресурс] / Дар'я Денисова // Focus.ua : [вебсайт]. – 2025. – 9 лип. – Електрон. дані. *Як підтвердив перший заступник міністра фінансів Денис Улютін під час засідання Комітету Верховної Ради України (ВР України) з питань фінансів, податкової та митної політики, розкриття банківської таємниці в Україні буде. Наразі розглядається законопроєкт № 13233 про створення реєстру банківських рахунків та сейфів фізичних осіб. Розглянуто, що саме прописано в цьому Законі та чи не порушує він прав українців, яку інформацію про клієнтів планують надавати банки. За словами експертів, законопроєкт покликаний вирівняти законодавство України з євростандартами, але викликає серйозні дискусії про конституційні права і безпеку приватних даних.* Текст: <https://focus.ua/uk/economics/713663-bankivsku-tayemnicyu-rozkriyut-hto-teper-pobachit-rahunki-ukrajinciv>
4. **Для чого збирають персональні дані** [Електронний ресурс] / Прес-служба Апарату Верхов. Ради України // Голос України. – 2025. – 11 лип.   
   (№ 387. – Електрон. дані. *Омбудсман України Дмитро Лубінець зазначив, що громадяни мають право знати, навіщо збирають їхні персональні дані і на якій підставі це роблять. Захист таких даних гарантують Конституція України та Закон України «Про захист персональних даних». Склад і зміст персональних даних мають бути відповідними, адекватними та не надмірними для конкретної мети їх обробки. Наголошено, що громадянин має право подати запит і отримати, крім випадків, передбачених законом, інформацію про те, які саме дані про нього збирають, навіщо та на якій підставі. Для цього в запиті потрібно вказати прізвище, ім’я та по батькові, місце проживання або перебування, а також реквізити документа, що підтверджує особу. Зауважено, що протягом 10 робочих днів із дня надходження запиту власник персональних даних повідомить, чи буде запит задоволено, або ж надасть обґрунтування правових підстав для відмови. Запит задовольняється протягом 30 календарних днів із дня його надходження.* Текст: <https://www.golos.com.ua/article/385126>
5. **Залата О. Обдурить і підставить: у яких випадках небезпечно використовувати ChatGPT та інших ботів із ШІ** [Електронний ресурс] / Олександр Залата // Focus.ua : [вебсайт]. – 2025. – 1 лип. – Електрон. дані. *Зазначено, що моделі штучного інтелекту (ШІ), як-от ChatGPT, мають обмеження, тому в них ризиковано запитувати інформацію кількох типів. Вказано, що чатбот може бути впевнений у своїй інформації, навіть якщо відверто неправий. Тож, коли питання стосується податків, медичних діагнозів, судових розглядів або банківських рахунків, помилка може коштувати дуже дорого. Журналіст видання «CNET» Нельсон Агілар поділився своїм досвідом того, коли краще не використовувати ШІ.* Текст: <https://focus.ua/uk/digital/712485-obdurit-i-pidstavit-u-yakih-vipadkah-nebezpechno-vikoristovuvati-chatgpt-ta-inshih-botiv-iz-shi>
6. **Зінченко М. Центр демократії та верховенства права презентував посібник «Медіа майбутнього: працюємо в часи змін»** [Електронний ресурс] / Мар’яна Зінченко // Детектор медіа : [інтернет-вид.]. – 2025. – 30 лип. – Електрон. дані. *Вказано, що презентований посібник покликаний допомогти журналістам і працівникам медіа адаптуватися до сучасних викликів. Він орієнтований на журналістів, редакторів, медіаменеджерів і всіх, хто працює в інформаційному середовищі. У виданні зібрано практичні поради та інструменти, зокрема щодо: захисту прав і персональних даних медійників; боротьби з дезінформацією; безпечного й етичного використання штучного інтелекту (ШІ) у журналістській роботі. Посібник розроблено за підтримки International Media Support (IMS).* Текст: <https://detector.media/infospace/article/243038/2025-07-30-tsentr-demokratii-ta-verkhovenstva-prava-prezentuvav-posibnyk-media-maybutnogo-pratsyuiemo-v-chasy-zmin/>
7. **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.*
8. **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>
9. **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>
10. **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>
11. **Члени української парламентської делегації взяли участь у заході літньої сесії ПА ОБСЄ щодо протидії російській дезінформації** [Електронний ресурс] / Прес-служба Апарату Верхов. Ради України // Голос України. – 2025. – 2 лип. (№ 380). – Електрон. дані.*Подано інформацію, що у межах літньої сесії Парламентської Асамблеї ОБСЄ (Порту, Португалія) відбувся окремий тематичний захід (side event), присвячений викликам, пов’язаним із російською дезінформацією та пропагандою як елементом гібридної війни. У ньому взяли участь парламентарі з багатьох країн світу, представники громадянського суспільства, експерти з питань інформаційної безпеки, а також українські та іноземні спікери. Заступниця голови Комітету Верховної Ради України (ВР України) з питань гуманітарної та інформаційної політики Євгенія Кравчук зауважила, що російська пропаганда та втручання у демократичні процеси – це не лише проблема України. Це пряма загроза для безпеки та стабільності демократичних суспільств Європи, зокрема через втручання у вибори. У своєму виступі Є. Кравчук акцентувала на необхідності створення «інформаційного Рамштайну» – міжнародної координаційної платформи для обміну інформацією, ініціативами та спільними діями у сфері протидії дезінформації. Вона переконана, що сьогодні нам так само потрібно запроваджувати персональні санкції і відповідальність проти російських пропагандистів і організаторів дезінформаційних кампаній, які, по суті, працюють на розпалювання ненависті та виправдання геноциду українців.* Текст: <https://www.golos.com.ua/article/384983>

**Підготовлено відділом інформаційного забезпечення органів влади**

**Національної бібліотеки України імені Ярослава Мудрого**

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

**31.07.2025**