**Кібербезпека**

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

***анотований бібліографічний список***

***2024. – Вип. 5 (травень). – 10 с.***

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

1. **Андрусяк А. В Україні запустять додаток «Армія+»: у Міноборони розповіли, навіщо він потрібен військовим** [Електронний ресурс] / Анастасiя Андрусяк В // Focus.ua : [вебсайт]. – 2024. – 24 трав. – Електрон. дані. *Як заявив офіцер Збройних сил України (ЗСУ) та голова управління інформаційних технологій (IT) в Міністерстві оборони України (МО України) Олег Берестовий, для українських військовослужбовців запустять додаток «Армія+», покликаний спростити низку процесів. Зазначено, що у сервісі будуть доступні електронні рапорти, навчання, документи, сертифікати, нагороди та інші функції. Очікується, що нові опції з'являтимуться регулярно. За словами О. Берестового, подібні технології та сервіси є «цифровими інструментами турботи» про українських військовослужбовців, майбутніх військовослужбовців і ветеранів. Заступниця міністра оборони України з цифровізації Катерина Чорногоренко повідомила, що «Армія+» розробляється МО України спільно з Міністерством цифрової трансформації України: є юридичний відділ, який займається нормативно-правовими актами, команда бізнес-аналітиків, продуктова команда, яка безпосередньо розробляє застосунок, а також команда кіберфахівців, які дбають про протоколи захисту*. Текст: <https://focus.ua/uk/digital/648286-dodatok-armiya-koli-z-yavitsya-i-navishcho-potriben>
2. **Андрусяк А. На рівні з супутниками і БПЛА: як чат-бот «єВорог» допомагає нищити ЗС РФ, – Мінцифри** [Електронний ресурс] / Анастасія Андрусяк // Focus.ua : [вебсайт]. – 2024. – 3 трав. – Електрон. дані. *Йдеться про офіційний чат-бо «єВорог», створений Міністерством цифрової трансформації України. Розглянуто, як зараз працює сервіс і чому він такий важливий для українців. За словами представника відомства, «єВорог» є одним із важливих елементів боротьби з окупантами. Українці подають у чат-бот заявки з інформацією про розміщення російських військ, які проходять два етапи верифікації. Далі інформація потрапляє на карти ситуаційної обізнаності та автоматизованого ведення бою, якими користуються Сили оборони України. Там ці дані додатково верифікуються за іншими джерелами, серед яких: бот Служби безпеки України (СБУ), дрони, поліція, розвідка, камери спостереження, а також люди, які телефонують на гарячу лінію.*  Текст: <https://focus.ua/uk/eksklyuzivy/644324-na-rivni-z-suputnikami-i-bpla-yak-chat-bot-yevorog-dopomagaye-nishchiti-zs-rf-mincifri>
3. **Андрусяк А. «Telegram небезпечний»: в Україні пропонують створити месенджер на базі «Дії»** [Електронний ресурс] / Анастасія Андрусяк // Focus.ua : [вебсайт]. – 2024. – 13 трав. – Електрон. дані. *За повідомленням «Детектор медіа» з посиланням на представників Громадської організації (ГО) «Аналітичний центр інформаційних ресурсів», українські волонтери, які створили застосунок для перевірки конфіденційності в месенджері «Telegram», запропонували створити захищений сервіс комунікацій на базі застосунку «Дія». Зазначено, що в такий спосіб українці зможуть отримувати інформацію від офіційних відомств, наприклад, Офісу Президента України (ОПУ), Генерального штабу Збройних сил України (ЗСУ), а також від медіа та ГО. При цьому представники влади, медіа та громадські діячі отримають безпечний канал комунікації. Аналітик організації Богдан Соломикін зазначив, що жоден додаток не може бути безпечним на 100 %. Усі дані, які потрапляють у мережу, можуть з'являтися у відкритому доступі. При цьому в умовах війни найбільше запитань викликає «Telegram». За словами аналітика, організація провела дослідження і з'ясувала, що після видалення з «Telegram» інформація зберігається ще кілька годин.*  Текст: <https://focus.ua/uk/digital/646244-telegram-nebezpechniy-v-ukrajini-proponuyut-stvoriti-mesendzher-na-bazi-diji>
4. **Бодунова О. М. Теоретико-прикладні основи запобігання злочинності у сфері інформаційних технологій** / Олеся Миколаївна Бодунова ; М-во фінансів України, Держ. податк. ун-т. – Луцьк : Вежа-Друк, 2023. – 341 с. : табл. ***Шифр зберігання в Бібліотеці:* *Б372280*** *У монографії висвітлено поняття інформаційної безпеки як одного з основних напрямів кримінологічної політики України. Визначено стан наукових досліджень злочинності у сфері інформаційних технологій. Подано наукове уявлення про сучасний стан злочинності у цій сфері. Сформовано кримінологічний портрет особи злочинця, що вчиняє кримінальні правопорушення у сфері інформаційних технологій, охарактеризовано види кримінальних правопорушень. Висвітлено нормативно-правове забезпечення запобігання цьому виду злочинності, зокрема в умовах воєнного стану в Україні.*
5. **Бурдейна О. «Можуть злити в Інтернет»: експерт визнав проблему захищеності застосунку «Резерв+» (відео)** [Електронний ресурс] / Олена Бурдейна // Focus.ua : [вебсайт]. – 2024. – 21 трав. – Електрон. дані. *Зазначено, що в Міністерстві оборони України (МО України) у межах мобілізації в Україні створили застосунок «Резерв+», який містить чутливі дані і слабко захищений від проникнення ззовні. Про деталі роботи мобільної програми для військового обліку повідомив експерт із кібербезпеки Костянтин Корсун. За його словами, застосунок дійсно створили на основі електронного шкільного щоденника, і це припустимо. Однак складається враження, що його робили надто швидко і не потурбувались про безпеку даних. Експерт також розповів, як можуть діяти російські спецслужби, якщо викрадуть дані про українських військовослужбовців.*  Текст: <https://focus.ua/uk/voennye-novosti/647731-mobilizaciya-v-ukrajini-vimagaye-zahishchenosti-zastosunku-yakoji-nemaye-video>
6. **Гурко М. Анатолій Шинкарьов «Блокчейн: новий щит для українських солдатів від IT Freedom»** [Електронний ресурс] / Мирослав Гурко // Focus.ua : [вебсайт]. – 2024. – 3 трав. – Електрон. дані. *Засновник української IT корпорації «IT Freedom» Анатолій Шинкарьов прокоментував засадничі принципи та можливості застосування блокчейн-технології в умовах військового конфлікту, за допомогою якого можна забезпечити нескомпрометованість переданої інформації та її повноцінну безпеку. Однією з ключових переваг блокчейна в умовах військових дій є забезпечення прозорості та відстежуваності поставок. Зазначено, що у сучасних реаліях проблеми з логістикою можуть коштувати життів, але блокчейн дає змогу запобігти фальсифікаціям і поліпшити координацію між взаємодіючими вузлами зв'язку. Крім того, децентралізований характер блокчейна посилює безпеку військових комунікацій, захищаючи їх від перехоплення та атак. Кожне повідомлення шифрується таким чином, що його може прочитати тільки адресат. Проте однією з ключових переваг є можливість економічного застосування в постачанні та фінансовій підтримці України з боку країн-партнерів і незалежних осіб. Вказано, що «IT Freedom» – це компанія, фокусом якої є розробка блокчейн-технологій і рішень, що охоплює весь спектр послуг, з акцентом на децентралізацію бізнесу і кібербезпеку.*  Текст: <https://focus.ua/uk/technologies/644194-anatoliy-shinkarov-blokcheyn-noviy-shchit-dlya-ukrajinskih-soldativ-vid-it-freedom>
7. **Думчиков М. О. Концептуальні засади кримінально-правової охорони кіберпростору в Україні** / Михайло Олександрович Думчиков ; М-во освіти і науки України, Сум. держ. ун-т. – Суми : Сум. держ. ун-т, 2023. –
412 с. : іл. ***Шифр зберігання в Бібліотеці: А831025*** *У монографії розкрито сутність та різновиди кримінальних правопорушень у кіберпросторі**та запропоновано науково й теоретично обгрунтовані підходи до вдосконалення кримінального законодавства щодо встановлення кримінальної відповідальності за такі правопорушення. Особливу увагу приділено кваліфікації кримінальних правопорушень, передбачених XVI розділом Особливої частини Кримінального кодексу України. Типологізовано кримінальні правопорушення в кіберпросторі. Акцентовано увагу на аналізі міжнародних конвенцій, що визначають відповідальність за суспільно небезпечні діяння, вчинені в кіберпросторі. Проаналізовано стан імплементації норм Конвенції «Про кіберзлочинність» у національне законодавство України.*
8. **Євдокимов С. О. Сучасні системи захисту інформації** / Сергій Олександрович Євдокимов. – Київ : Гуляєва В. М., 2023. – 378 с. : іл., табл. ***Шифр зберігання в Бібліотеці: В83279*** *Розкрито можливості використання сучасних програм для виявлення несанкціонованого втручання в роботу електронного документообігу та запобігання витоку інформації в локальній мережі підприємства. Надано характеристики каналів витоку інформації на підприємстві. Запропоновано засоби програмного захисту інформації в LAN. Наведено поради з практичного використання антивірусних програм; відновлення видаленої інформації та цілісності інформації; резервного копіювання інформації та безпеки даних. Розглянуто охорону праці та безпеки в надзвичайних ситуаціях. Проаналізовано міжнародні стандарти до Охорони праці з ЕОМ, відповідні умови для праці та супроводження ЕОМ. Приділено увагу безпеці в цифровому середовищі та кібергігієні.*
9. **Зінченко М. Шахраї під час вимкнень світла крадуть акаунти та поширюють дезінформацію через фейкові чат-боти – Міненерго** [Електронний ресурс] / Мар’яна Зінченко // Детектор медіа : [інтернет-вид.]. – 2024. – 24 трав. – Електрон. дані.*Йдеться про попередження**Міністерства енергетики України щодо активізації шахраїв у зв'язку з відключенням електроенергії. За даними відомства, у період відключення світла шахраї створюють фейкові чат-боти енергетичної компанії, через які викрадають облікові записи клієнтів і крадуть гроші. Також вони поширюють дезінформацію. У Міненерго зазначили, що минулого року кіберполіція викрила групу таких шахраїв. Міністерство закликає не довіряти стороннім ресурсам і не переходити за посиланнями з незнайомих джерел. Достовірну інформацію про ситуацію в енергосистемі та відключення можна отримати на ресурсах Міненерго, НЕК «Укренерго» та операторів системи розподілу (обленерго) в областях.* Текст: <https://ms.detector.media/kiberbezpeka/post/35021/2024-05-24-shakhrai-pid-chas-vymknen-svitla-kradut-akaunty-ta-poshyryuyut-dezinformatsiyu-cherez-feykovi-chat-boty-minenergo/>
10. **Калайда Ю. П.** **Агресія рф у кіберпросторі як загроза національній безпеці України** [Електронний ресурс] / Ю. П. Калайда// Інформація і право. – 2024. – № 1. – С. 188-194. *Проаналізовано* *агресію РФ у кіберпросторі. Висвітлено історію кібервійни України з РФ, виділено її ознаки і етапи. Проаналізовано законодавство України у сфері забезпечення кібербезпеки. Внесено пропозиції щодо напрямів реформування сектора безпеки і оборони у цій сфері, а також реалізації законодавчих ініціатив у сфері протидії кібератакам. Наголошено на необхідності якнайшвидшого створення та функціонування кібервійськ у складі Збройних сил України (ЗСУ).*  Текст: <http://il.ippi.org.ua/article/view/300810>
11. **Катишев К. Україна підписала безпекову угоду з Бельгією** [Електронний ресурс] / Костянтин Катишев // Korrespondent.net : [вебсайт]. – 2024. – 28 трав. – Електрон. дані*. Зазначено, що Президент України Володимир Зеленський і прем’єр-міністр Бельгії Александр Де Кроо підписали у Брюсселі двосторонню угоду про співробітництво у сфері безпеки та довгострокову підтримку. Згідно з угодою Бельгія виділить Україні на військову допомогу щонайменше 977 млн євро цього року та  надаватиме підтримку Україні протягом 10-річного терміну дії угоди. Також Бельгія гарантує, що надаватиме своєчасну безпекову допомогу, сучасну військову техніку та озброєння з урахуванням потреб України у сфері ВПС і ППО, морської безпеки, розмінування та в межах коаліції з питань боєприпасів і сприятиме проведенню військових тренувань; поглиблюватиме співпрацю у сферах розвідки, кібербезпеки та протидії дезінформації тощо.* Текст: <https://ua.korrespondent.net/ukraine/4690063-ukraina-pidpysala-bezpekovu-uhodu-z-belhiieui>
12. **Конституція України: стан, перспективи та механізми реалізації** : [матеріали] Всеукр. наук.-практ. конф., 27 черв. 2023 р. / НАН України, Київ. ун-т права ; [за заг. ред.: Ю. Л. Бошицький]. – Вінниця : Твори, 2023. – 347 с. ***Шифр зберігання в Бібліотеці:*  *Б371303*** *Зі змісту:**Конституційна модернізація права на свободу думки і слова, на вільне вираження своїх поглядів і переконань з метою запобігання кіберзлочинності / І. Харитоненко. – С. 312-318.*
13. **Микитюк В. путін планує «фізичні атаки» на Захід: що про це відомо**[Електронний ресурс] / Вікторія Микитюк // Fakty.ua : [вебсайт]. – 2024. – 17 трав. – Електрон. дані. *Як заявила глава Центру урядового зв'язку Британії Анна Кіст-Батлер, РФ прагне піти далі, ніж просто атаки в кіберпросторі. Агентство зв'язку «дедалі більше занепокоєне зростаючими зв'язками між російськими спецслужбами і проксі-групами для проведення кібератак, а також підозрами у фізичному спостереженні і саботажних операціях». Наголошено, що РФ вже давно звинувачують у тому, що вона захищає кібер-банди, які націлені на західні організації, дозволяючи їм діяти відносно безкарно, здійснюючи складні хакерські атаки*. Текст: <https://fakty.ua/437700-putin-planiruet-fizicheskie-ataki-na-zapad-chto-ob-etom-izvestno>
14. **Новий проєкт кіберполіції: чатові онлайн** [Електронний ресурс] // Юрид. газ. – 2024. – 20 трав. – Електрон. дані. *За повідомленням, начальника відділу управління протидії кіберзлочинам у м. Києві, майора поліції Олега Дубіна, чатові онлайн – це проєкт, який входить до екосистеми «BRAMA», створений волонтерами та небайдужими громадянами за підтримки Департаменту кіберполіції, головною ідеєю якого є протидія інформаційній експансії ворога. Вебсайт «Чатові онлайн» створено як альтернативу Telegram, який об’єднуватиме декілька напрямків діяльності для більшого зацікавлення та залученості користувачів. Вебсайт «Чатові онлайн» розробляється Ukrainian IT HUB за підтримки Акселераційної програми Act to Support проєкту «Фенікс», що виконується Фондом Східна Європа коштом Європейського Союзу (ЄС). Екосистема «BRAMA» спрямована на захист медіапростору від російської пропаганди, блокування каналів поширення дезінформації, протиправного та забороненого контенту. Також метою проєкту є покращання медіаграмотності українців, зменшення впливу пропаганди на суспільство та популяризація безпечного поводження в інтернеті.* Текст: <https://yur-gazeta.com/golovna/noviy-proekt-kiberpoliciyi-chatovi-onlayn.html>
15. **Поліковська Ю.** **Україна і Польща підписали меморандум про співпрацю у цифровій галузі, – AIN.ua** [Електронний ресурс] / Юлія Поліковська // Детектор медіа : [інтернет-вид.]. – 2024. – 6 трав. – Електрон. дані.  *Повідомлено, що віцепрем’єр-міністр і міністр цифрової трансформації Польщі Кшиштоф Гавковський 6 травня здійснив робочий візит до Києва та зустрівся із віцепрем’єр-міністром і міністром цифрової трансформації України Михайлом Федоровим. Сторони підписали меморандум про співпрацю в цифровій галузі двох держав. Вказано ключові моменти візиту: Польща пообіцяла Україні допомогу у забезпеченні доступу до інтернету в Україні, зокрема власне забезпечення системами Starlink. Сторони домовилися забезпечити довгострокові механізми кібербезпеки. Польща підтвердила свою підтримку України, зазначивши, що обсяг допомоги становить 2,5 % її річного ВВП, що робить її одним із лідерів серед країн-донорів. Зауважено, що у Польщі зараз локалізовані сервери підтримки українських підприємств і держава задекларувала готовність надалі забезпечувати безпеку цих даних. Польський віцепрем’єр також запросив Федорова з візитом до Польщі, щоб поділитися досвідом та успіхами України у цифровій трансформації.* Текст: <https://ms.detector.media/internet/post/34849/2024-05-06-ukraina-i-polshcha-pidpysaly-memorandum-pro-spivpratsyu-u-tsyfroviy-galuzi-ainua/>
16. **Савінцев С. Озброєна штучним інтелектом: РФ є найбільшою загрозою для виборів у США, – The Hill** [Електронний ресурс] / Сергій Савінцев // Focus.ua : [вебсайт]. – 2024. – 16 трав. – Електрон. дані. *Як повідомило видання «The Hill», РФ, Китай та Іран намагатимуться вплинути на майбутні вибори в США, цього разу використовуючи останні інновації в галузі штучного інтелекту (ШІ) для поширення дезінформації в Інтернеті, введення в оману виборців і підриву довіри до демократії. Вказано, що останнє попередження американських спецслужб пролунало щодо створення ШІ реалістичних зображень, відео- та аудіоматеріалів, здатних обдурити навіть найвибагливішого виборця. Зокрема, останніми місяцями РФ вхопилася за американські дебати щодо імміграції, поширюючи пости, які перебільшують вплив міграції, вочевидь, намагаючись викликати обурення серед американських виборців. Крім того, інструментами дезінформації є державні засоби масової інформації (ЗМІ), онлайн-інфлюенсери та мережі фейкових акаунтів, які можуть швидко поширювати неправдивий і оманливий контент. Окрім того, в США припускають, що супротивник може зламати виборчі системи штатів або місцевих органів влади, щоб змінити результати голосування або створити враження, що результатам виборів не можна довіряти.* Текст: <https://focus.ua/uk/world/646694-ozbroyena-shtuchnim-intelektom-rf-ye-naybilshoyu-zagrozoyu-dlya-viboriv-u-ssha-the-hill>
17. **Савінцев С. У перші дні роботи «Резерв+» зазнав кількох потужних кібератак, – Міноборони** [Електронний ресурс] / Сергій Савінцев // Focus.ua : [вебсайт]. – 2024. – 27 трав. – Електрон. дані. *Як повідомила заступниця міністра оборони з питань цифрового розвитку, цифрових трансформацій і цифровізації Катерина Черногоренко, у перші два дні після запуску застосунку «Резерв+» на нього було здійснено кілька потужних кібератак, що викликало певні незручності. За її словами, Міністерство оборони України (МО України) було готове до того, що ворог намагатиметься зірвати роботу застосунку «Резерв+» та запустить DDоS-атаки.* Текст: <https://focus.ua/uk/digital/648810-u-pershi-dni-roboti-rezerv-zaznav-kilkoh-potuzhnih-kiberatak-minoboroni>
18. **Ткачук Н. А. Досвід США зі створення та розбудови Кіберкомандування: уроки для України** [Електронний ресурс] / Н. А. Ткачук // Інформація і право. – 2024. – № 1. – С. 139-149. *Досліджено досвід США як країни, яка має найпотужніші кіберспроможності у світі зі створення, забезпечення функціонування та розвитку Кіберкомандування, у контексті можливості використання зазначеного досвіду Україною під час розбудови власних кіберсил.* Текст:<http://il.ippi.org.ua/article/view/300798>
19. **Федієнко О. П.** **Сучасні тенденції нормативного забезпечення інституційного формування кібервійськ (кіберсил): досвід деяких країн НАТО** [Електронний ресурс] / О. П. Федієнко // Інформація і право. – 2024. – № 1. – С. 150-161. *Проаналізовано нормативні документи, присвячені створенню кібервійськ у країнах-членах НАТО (Великобританія, США). Розглянуто компетенцію, повноваження та функціональні завдання практичної діяльності кіберпідрозділів. Узагальнено особливості використання кібервійськ у межах проведення оборонних і наступальних кібероперацій. Окреслено зміст і значення доктрини когнітивного ефекту та наслідків її використання. Деталізовано здобутки та приклади успішної діяльності кібервійськ Великобританії та США. На підставі узагальнення позитивного зарубіжного досвіду створення кібервійськ окреслено перспективи законодавчого забезпечення інституційного утворення кіберсил в Україні.* Текст: <http://il.ippi.org.ua/article/view/300800>
20. **Як не стати жертвою шахраїв та ворожої пропаганди: в кіберполіції розповіли про фактчекінг** [Електронний ресурс] // Юрид. газ. – 2024. – 6 трав. – Електрон. дані.*Зазначено: щоб* *не стати жертвою пропаганди чи шахраїв, необхідно переконуватися у достовірності інформації. Фахівці Департаменту кіберполіції Національної поліції України (НПУ) розповіли про те, як відбувається перевірка інформації на достовірність.**Йдеться про**фактчекінг – процес перевірки достовірності фактів, інформації та тверджень, які поширюються в медіа, соціальних мережах та інших медійних джерелах. Цей інструмент використовується для: виявлення неправдивої інформації та спростування фейкових новин, пропаганди та дезінформації; підтвердження достовірності інформації для допомоги людям у прийнятті обґрунтованих рішень на основі фактів; підвищення рівня прозорості медіапростору. Розглянуто, як використовувати фактчекінг.* Текст:[https://yur-gazeta.com/golovna/yak-ne-stati-zhertvoyu-shahrayiv-ta-vorozhoyi-propagandi-v-kiberpoliciyi-rozpovili-pro-faktcheking.htm](https://yur-gazeta.com/golovna/yak-ne-stati-zhertvoyu-shahrayiv-ta-vorozhoyi-propagandi-v-kiberpoliciyi-rozpovili-pro-faktcheking.html)

**Підготовлено відділом інформаційного забезпечення органів влади**

**Національної бібліотеки України імені Ярослава Мудрого**

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

**31.05.2024**