УДК 343.9:004.056
DOI https://doi.org/10.24144/2307-3322.2025.87.3.41

ПРОФІЛАКТИКА КІБЕРЗЛОЧИНІВ В УМОВАХ ЦИФРОВІЗАЦІЇ ДЕРЖАВНОГО УПРАВЛІННЯ ТА БІЗНЕСУ

Дмитрів С.О.,
старший викладач кафедри права та фінансів
Луцького інституту розвитку людини Університету «Україна»
ORCID: 0000-0002-0087-706X

Пікалюк С.С.,
старший викладач кафедри права та фінансів
Луцького інституту розвитку людини Університету «Україна»
ORCID: 0000-0001-7035-9527

Дмитрів С.О., Пікалюк С.С. Профілактика кіберзлочинів в умовах цифровізації державного управління та бізнесу.

Стаття присвячена аналізу кіберзлочинності, що виникає в умовах цифровізації державного управління та бізнесу. У роботі розглядаються основні типи кіберзлочинів, що становлять найбільшу загрозу для державних структур і бізнесу, а також заходи, які можуть бути застосовані для їх профілактики. Особлива увага приділяється розвитку цифрових технологій в Україні та впливу цього процесу на зростання кіберзагроз. Цифровізація надає численні переваги для ефективності управлінських процесів і розвитку бізнесу, однак разом із цими можливостями з'являються й нові ризики, зокрема у вигляді кіберзлочинності. Відзначається, що кіберзлочини стають дедалі складнішими, охоплюючи порушення роботи інформаційних систем, викрадення даних, фінансові махінації, фішинг, а також криптовалютні шахрайства. Це зумовлює потребу у вдосконаленні механізмів кіберзахисту на рівні державних органів та бізнес-структур. Значну роль у зростанні кіберзлочинності відіграє поширення складних методів атак, що використовують штучний інтелект, соціальну інженерію та автоматизовані алгоритми для злому інформаційних систем. Злочинці дедалі частіше орієнтуються не лише на великі корпорації та урядові установи, а й на малий та середній бізнес, що часто має обмежені можливості для ефективного захисту. Крім того, цифрові загрози не обмежуються лише економічними втратами – вони можуть мати суттєві наслідки для національної безпеки, соціальної стабільності та довіри громадян до цифрових сервісів. Саме тому нагальною є необхідність впровадження комплексних механізмів кібербезпеки, що включають не лише технічні засоби захисту, а й підвищення обізнаності користувачів про можливі ризики та методи їх уникнення. Стаття також акцентує увагу на необхідності розробки системи превентивних заходів для протидії кіберзлочинності, яка включає як технічні, так і організаційні та правові аспекти. Зокрема, пропонуються практичні рекомендації щодо підвищення стійкості інфраструктури державного управління та бізнесу до кіберзагроз, а також визначаються основні напрямки для покращення правового регулювання в сфері кібербезпеки. В умовах цифрової трансформації для України особливо важливою є інтеграція в міжнародні ініціативи, спрямовані на боротьбу з кіберзлочинністю, зокрема через співпрацю з ЄС, НАТО та INTERPOL. Це дозволяє отримати доступ до передових практик і технологій, що допомагають забезпечити кібербезпеку на всіх рівнях суспільства. Таким чином, ефективна профілактика кіберзлочинності в умовах цифровізації потребує комплексного підходу, включаючи розвиток національних механізмів захисту інформації, підвищення цифрової грамотності та активну співпрацю з міжнародними партнерами для створення безпечного цифрового середовища.

Ключові слова: кіберзлочинність, цифровізація, державне управління, бізнес, кіберзахист, профілактика, інформаційні системи, кіберзагрози, криптовалютні шахрайства, фішинг, інформаційна безпека, цифрова трансформація.

Dmytriv S.O., Pikaliuk S.S. Prevention of cybercrime in the context of digitalisation of public administration and business.

The article is devoted to the analysis of cybercrime arising in the context of digitalisation of public administration and business. The paper discusses the main types of cybercrime that pose the greatest threat to government agencies and businesses, as well as measures that can be taken to prevent them. Special attention is paid to the development of digital technologies in Ukraine and the impact of this process on the growth of cyber threats. Digitalisation provides numerous benefits for the efficiency of management processes and business development, but along with these opportunities, new risks arise, in particular in the form of cybercrime. It is noted that cybercrime is becoming increasingly complex, covering disruption of information systems, data theft, financial fraud, phishing, and cryptocurrency fraud. This necessitates the improvement of cyber defence mechanisms at the level of government agencies and businesses. A significant role in the growth of cybercrime is played by the proliferation of sophisticated attack methods that use artificial intelligence, social engineering, and automated algorithms to hack into information systems. Criminals are increasingly targeting not only large corporations and government agencies, but also small and medium-sized businesses, which often have limited capacity to effectively defend themselves. In addition, digital threats are not limited to economic losses - they can have significant consequences for national security, social stability, and public trust in digital services. That is why there is an urgent need to introduce comprehensive cybersecurity mechanisms that include not only technical protection, but also raising awareness of users about possible risks and methods of avoiding them. The article also focuses on the need to develop a system of preventive measures to counter cybercrime, which includes both technical, organisational and legal aspects. In particular, the author offers practical recommendations for enhancing the resilience of public administration and business infrastructure to cyber threats, and identifies the main areas for improving legal regulation in the field of cybersecurity. In the context of digital transformation, it is particularly important for Ukraine to integrate into international initiatives aimed at combating cybercrime, in particular through cooperation with the EU, NATO and INTERPOL. This allows access to best practices and technologies that help ensure cybersecurity at all levels of society. Thus, effective prevention of cybercrime in the context of digitalisation requires a comprehensive approach, including the development of national information security mechanisms, raising digital literacy and active cooperation with international partners to create a secure digital environment.

Key words: cybercrime, digitalisation, public administration, business, cyber defence, prevention, information systems, cyber threats, cryptocurrency fraud, phishing, information security, digital transformation.

Постановка проблеми. Сучасна цифровізація охоплює всі аспекти життєдіяльності, включаючи державне управління та бізнес, відкриваючи нові можливості для автоматизації, підвищення ефективності та розширення доступу до послуг. Водночас вона створює нові виклики, зокрема кіберзлочинність, яка загрожує інформаційним системам, економічній стабільності та суспільній безпеці. Кіберзлочини стають дедалі складнішими, спрямованими на викрадення даних, фінансові махінації та порушення функціонування державних і бізнес-структур. В Україні, яка перебуває в умовах трансформаційних змін і постійних кібератак, це питання набуває особливої актуальності.

Вивчення причин кіберзлочинності та розробка ефективних профілактичних заходів є необхідними для забезпечення інформаційної та економічної безпеки держави і бізнесу.

Метою даного дослідження є аналіз загроз кіберзлочинності, які виникають у процесі цифровізації державного управління та бізнесу, а також розробка ефективних рекомендацій щодо їх профілактики.

Стан опрацювання проблематики. Проблема профілактики кіберзлочинності в умовах цифровізації державного управління та бізнесу активно досліджується як в Україні, так і за кордоном. Українські науковці, зокрема Д.С. Азаров і О.О. Берназюк, акцентують увагу на вразливості інформаційних систем державного і приватного секторів, а також на необхідності гармонізації національного законодавства з міжнародними стандартами. У працях І.Г. Гончаренка та О.Ж. Скибун розглядаються основні загрози, як-от фішинг, криптовалютні шахрайства та DDoS-атаки, і пропонуються шляхи підвищення кіберзахисту через цифрову грамотність та інноваційні технології. Міжнародні дослідження наголошують на важливості співпраці держав у боротьбі з кіберзлочин-

ністю в рамках ініціатив НАТО, ЄС та INTERPOL. Особливу увагу приділяють використанню штучного інтелекту для моніторингу загроз і розробки стратегій кіберзахисту.

Попри значну кількість досліджень, питання профілактики кіберзлочинності потребує подальшого вивчення, особливо з огляду на специфіку викликів в Україні. Це вимагає впровадження ефективних заходів і інтеграції міжнародного досвіду

Виклад основного матеріалу. Прогрес у цифровізації державного управління та бізнесу відкриває нові можливості, проте формує й нові загрози, зокрема кіберзлочинність, яка стає дедалі витонченішою. Цифровізація змінює характер злочинності, створюючи вразливості через інтеграцію технологій у повсякденне життя. Це вимагає аналізу впливу технологій на появу нових типів кіберзлочинів, вразливих сфер та ефективних заходів їх профілактики [17, с. 15–19].

Україна перебуває на етапі активної цифрової трансформації, яка охоплює державний і приватний сектори. Впровадження електронного урядування, зокрема платформи «Дія», спрощує доступ до послуг і підвищує прозорість управління. У бізнесі цифровізація проявляється зростанням електронної комерції, автоматизацією процесів та використанням хмарних технологій, CRM-систем і IT-інфраструктур для аналізу даних та управління.

Однак, попри активний розвиток цифрових технологій, Україна стикається з низкою проблем. Серед них – нерівномірність доступу до цифрових інструментів між різними регіонами, недостатній рівень цифрової грамотності значної частини населення та низька захищеність багатьох інформаційних систем від кіберзагроз [3, с. 45–52]. Це створює серйозні виклики для забезпечення ефективності цифровізації та її безпечності як у державному секторі, так і у сфері бізнесу.

Цифровізація в Україні модернізує державне управління та бізнес, підвищуючи ефективність і створюючи нові можливості. Однак швидке впровадження технологій випереджає розвиток систем захисту, що робить установи й бізнес вразливими до кіберзлочинів. Це вимагає аналізу типів таких злочинів, їхньої специфіки та впливу на ключові сфери діяльності [2, с. 207]. Серед найпоширеніших типів таких злочинів можна виокремити:

Кібератаки на державні системи та бізнес-інфраструктуру загрожують цифровому середовищу, спричиняючи економічні збитки, дискредитацію управління та порушення роботи організацій. Атаки типу DDoS і віруси, як-от Petya/NotPetya, завдають значної шкоди державним і приватним установам.

З розвитком електронного урядування зростають випадки **несанкціонованого доступу до персональних** даних через фішинг, шкідливі програми чи злами баз. Це загрожує фінансовими втратами, крадіжкою особистості та маніпуляцією інформацією.

Фінансові шахрайства в електронному середовищі включають злами банківських систем, підробку транзакцій, фішинг та шахрайства з криптовалютами. Ці загрози супроводжують цифровізацію й потребують ефективних заходів для захисту держави, бізнесу та громадян.

Однією з основних вразливостей державного сектору є **недосконаліть захисту даних**, яка полягає у використанні застарілих систем, недостатньому оновленні програмного забезпечення та слабкій інтеграції сучасних технологій безпеки [1, с. 20–29]. Наприклад, багато державних органів все ще використовують програми, які не мають належного рівня захисту, що робить їх вразливими до атак зловмисників. Зокрема, нерідко відсутні комплексні системи моніторингу кіберзагроз, які могли б виявляти атаки на ранніх стадіях.

Низька обізнаність працівників державних установ щодо кіберзагроз і **відсутність чітких стратегій реагування на атаки** підвищують ризик несанкціонованого доступу до даних, порушення роботи органів та зниження довіри громадян. Подолання цих проблем вимагає впровадження технічних рішень, підвищення цифрової грамотності та розробки ефективних стратегій кіберзахисту.

Бізнес також стикається з численними проблемами у сфері кібербезпеки, зокрема через недостатній рівень захисту інформаційних систем і зростання ризиків, пов'язаних із віддаленою роботою [8]. Ці аспекти, доповнені слабкою організаційною підготовкою та низьким рівнем кіберграмотності, посилюють вразливість бізнесу до атак і потребують детального аналізу та вирішення.

Ключовими проблемами бізнесу у сфері кібербезпеки є недооцінка важливості захисту даних, використання застарілого програмного забезпечення, відсутність шифрування та багаторівневої аутентифікації. Це створює прогалини в захисті, які зловмисники можуть легко використати. Додаткові ризики виникають через поширення віддаленої роботи, яка часто базується на менш захищених домашніх мережах, що посилює вразливість корпоративних систем [6, с. 1–4].

Для бізнесу вирішення цих проблем вимагає комплексного підходу: інвестування у сучасні системи кіберзахисту, впровадження політик безпеки, проведення регулярних навчань для працівників, а також створення захищених умов для дистанційної роботи. Такий підхід дозволить мінімізувати ризики кіберзагроз і зберегти стійкість бізнесу у цифровому середовищі [18].

Україна неодноразово ставала об'єктом масштабних кібератак, що мали значний вплив на державний сектор, бізнес та суспільство. Найбільш резонансними прикладами є атаки вірусів типу **Petya/NotPetya**, які показали вразливість цифрової інфраструктури країни.

Атака вірусу Petya у червні 2017 року стала однією з найбільших в історії України, заблокувавши доступ до інформації на десятках тисяч пристроїв у державних установах, банках і компаніях. Вірус поширювався через зламане програмне забезпечення M.E.Doc, підкресливши вразливість локальних систем. Хоча зловмисники вимагали викуп у криптовалюті, метою атаки була дестабілізація економіки та державних систем.

Вірус NotPetya, модифікована версія Petya, мав масштабніший і руйнівніший вплив, знищуючи дані навіть після виплати викупу. Атака охопила державні установи, корпорації та інфраструктуру, паралізувавши роботу у понад 60 країнах світу та завдавши збитків на мільярди доларів. Інцидент підкреслив глобальну загрозу кіберзлочинності та потребу в міжнародній координації для її протидії..

Окрім Petya/NotPetya, Україна зазнала значних кібератак, зокрема вірус BlackEnergy у 2015 році, спрямований на енергетичний сектор, що спричинив збої у постачанні електроенергії, та атаки на Центральну виборчу комісію у 2014 році, спрямовані на порушення підрахунку голосів. Ці інциденти демонструють складність кібератак і їхній потенціал до дестабілізації цілих галузей економіки та державного управління [18].

Ефективна протидія кіберзагрозам потребує не лише технічних рішень, але й вдосконалення нормативно-правової бази, яка визначає обов'язки держави, бізнесу та громадян у захисті інформації. Закон України «Про основні засади забезпечення кібербезпеки України» (2017) закладає принципи захисту в кіберпросторі, регулює повноваження суб'єктів кібербезпеки та питання захисту критичної інфраструктури, що є ключовими у профілактиці кіберзлочинів.

До основних правових аспектів, що сприяють профілактиці кіберзлочинів, належать:

– визначення статусу критичної інфраструктури. Законодавство зобов'язує власників об'єктів критичної інфраструктури впроваджувати заходи кібербезпеки, включаючи регулярний моніторинг, аудит безпеки та розробку стратегій реагування на інциденти [12];

– посилення відповідальності за кіберзлочини. У Кримінальному кодексі України передбачені статті, які встановлюють відповідальність за несанкціоноване втручання в роботу інформаційних систем, створення та поширення шкідливого програмного забезпечення, а також порушення правил захисту інформації;

– міжнародне співробітництво. Україна є учасницею Будапештської конвенції про кіберзлочинність (2001 рік), що сприяє співпраці з іншими країнами у боротьбі з кіберзлочинами, зокрема у сфері обміну інформацією та спільного розслідування інцидентів;

– розвиток спеціалізованих органів. В Україні створено спеціальні підрозділи, відповідальні за кібербезпеку, такі як Департамент кіберполіції Національної поліції України та Державний центр кіберзахисту при Державній службі спеціального зв'язку та захисту інформації.

Однак, попри прогрес у законодавчому регулюванні, залишаються певні проблеми, які потребують уваги. Це, зокрема, недостатня гармонізація національного законодавства з міжнародними стандартами, відсутність чітких механізмів реалізації багатьох положень закону та низький рівень виконання вимог щодо захисту інформаційних систем.

Подолання даних проблем потребує усвідомлення важливості адаптації до сучасних кіберзагроз на всіх рівнях суспільства. Ефективна профілактика кіберзлочинів значною мірою залежить від впровадження сучасних технологій кіберзахисту, які дозволяють оперативно виявляти загрози, мінімізувати ризики вторгнень та захищати критично важливу інформацію [5]. Серед ключових технічних заходів можна виділити наступні:

1. Використання антивірусних програм залишається базовим інструментом для захисту комп'ютерних систем від шкідливого програмного забезпечення, такого як віруси, трояни, шпигунські програми та програми-шифрувальники.

2. Системи **виявлення вторгнень (Intrusion Detection Systems)** та системи запобігання вторгненням (Intrusion Prevention Systems) забезпечують моніторинг мережевого трафіку для вияв-

лення підозрілої активності. IDS дозволяє фіксувати можливі загрози, тоді як IPS автоматично блокує такі дії до того, як вони завдадуть шкоди.

3. Використання міжмережевих екранів (Firewall) забезпечують контроль за доступом до мережі, фільтруючи вхідний та вихідний трафік на основі встановлених політик безпеки [11].

4. Шифрування даних є одним із найбільш надійних способів захисту конфіденційної інформації.

5. Системи резервного копіювання (Backup) дозволяють уникнути втрати інформації у разі атак шифрувальників чи інших інцидентів. Зберігання резервних копій у відокремлених і захищених середовищах є обов'язковою складовою стратегії кібербезпеки.

6. Автоматизовані системи моніторингу кіберзагроз. Сучасні рішення, що використовують штучний інтелект і машинне навчання, дозволяють аналізувати великі обсяги даних, виявляти аномальну активність та прогнозувати можливі загрози.

Впровадження цих технічних заходів є важливим кроком у забезпеченні кіберзахисту державного сектору та бізнесу [7]. Однак їх ефективність залежить від комплексного підходу, який включає як технічні, так і організаційні та правові заходи. Крім того, важливо забезпечувати регулярний аудит безпеки та адаптувати стратегії захисту відповідно до нових викликів.

Для забезпечення належного рівня кібербезпеки державні установи та компанії повинні створювати **спеціалізовані підрозділи**, відповідальні за моніторинг загроз, оновлення програмного забезпечення та реагування на інциденти. Також важливим є проведення **регулярних тренінгів для працівників**, оскільки людський фактор залишається однією з головних вразливостей у системах кіберзахисту [13].

Наявність детально розроблених **стратегій реагування на кіберзагрози** є важливою умовою мінімізації ризиків та наслідків кібератак. Такі стратегії повинні містити: чіткий розподіл ролей і відповідальності між членами команди під час інцидентів; порядок дій у разі виявлення кібератаки, включаючи заходи з ізоляції загроз та відновлення роботи систем; протоколи інформування керівництва, відповідних державних органів та клієнтів (за необхідності); план резервного копіювання та відновлення даних після атак [15].

Організаційні заходи є ключовими для формування ефективної системи кіберзахисту, яка потребує системності, регулярності та адаптації до змін. Україна активно співпрацює з міжнародними організаціями, такими як INTERPOL, ЄС та НАТО, що сприяє обміну інформацією, впровадженню передових практик та зміцненню національної безпеки. Взаємодія з партнерами дозволяє вдосконалювати захист критичної інфраструктури, розвивати професійний рівень фахівців та оперативно реагувати на загрози. Однак необхідно забезпечити гармонізацію законодавства з міжнародними стандартами, належне фінансування та ширшу участь у спільних проєктах [9].

Використання міжнародного досвіду дозволяє Україні вдосконалювати законодавчу базу, впроваджувати сучасні технології, розробляти ефективні протоколи реагування на кіберзагрози та навчати фахівців. Інтеграція цих практик сприятиме створенню надійної системи кіберзахисту, зниженню ризиків кіберзлочинів та зміцненню стійкості держави у цифровому середовищі [16, с. 48–53].

Основною перевагою спільної кібербезпекової платформи є оперативний обмін інформацією. У багатьох випадках кіберзлочини охоплюють кілька країн, що ускладнює їх розслідування та запобігання. Створення централізованої системи обміну даними про кібератаки, нові методи злочинців та вразливості дозволить країнам швидко реагувати на загрози. Наприклад, платформа може надавати аналітичні звіти, попередження про нові атаки та рекомендації для державних органів і бізнесу [14, с. 39–46].

Ще одним важливим аспектом є уніфікація стандартів кібербезпеки. Впровадження єдиних протоколів захисту інформації, тестування систем та сертифікації дозволить країнам забезпечити сумісність їхніх заходів безпеки. Це особливо актуально для захисту критичної інфраструктури, яка нерідко працює в умовах міжнародної кооперації [10].

Висновки. Проблема кіберзлочинності набуває все більшої актуальності в умовах цифровізації державного управління та бізнесу. Цифрова трансформація створює численні можливості для підвищення ефективності процесів, але водночас провокує появу нових загроз у сфері інформаційної безпеки. Злочинці активно використовують передові технології, такі як штучний інтелект, соціальна інженерія та криптовалютні транзакції, що ускладнює виявлення та протидію кіберзлочинам.

Аналіз основних типів кіберзлочинів показав, що найбільш поширеними є атаки на інформаційні системи, фінансові шахрайства, фішинг, криптовалютні афери та несанкціонований доступ до персональних даних. У зв'язку з цим виникає необхідність розробки комплексних заходів кіберзахисту, які включають технічні, організаційні та правові аспекти. Сучасні виклики вимагають впровадження передових технологій кібербезпеки, таких як багаторівнева автентифікація, шифрування даних, використання штучного інтелекту для моніторингу загроз та швидкого реагування на потенційні атаки.

Значну роль у протидії кіберзлочинності відіграє міжнародне співробітництво. Україна активно інтегрується у світові ініціативи у сфері кібербезпеки, співпрацюючи з ЄС, НАТО та INTERPOL. Обмін досвідом, участь у спільних проєктах та гармонізація законодавства з міжнародними стандартами сприяють зміцненню кіберзахисту на державному рівні та у бізнес-середовищі.

Таким чином, ефективна профілактика кіберзлочинності в умовах цифровізації вимагає комплексного підходу. Підвищення рівня цифрової грамотності, розвиток національних механізмів захисту інформації, впровадження сучасних технологій та активна міжнародна співпраця є ключовими напрямами забезпечення кібербезпеки в Україні. Лише об'єднання зусиль держави, бізнесу та громадянського суспільства дозволить створити безпечне цифрове середовище та мінімізувати ризики кіберзлочинності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Азаров Д.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис. канд. юрид. наук : 12.00.08. Київ, 2002. 246 с.
2. Бабанін С.В. Кіберзлочинність, Комп'ютерна злочинність. Велика українська юридична енциклопедія : у 20 т. Харків, 2019. Том 18. 544 с.
3. Берназюк О.О. Цифрові технології у праві: тенденції та перспективи розвитку : дис. д-ра юрид. наук: 12.00.07. Ужгород, 2021. 541 с.
4. Вісім найпопулярніших форм кіберзлочинів у інтернеті. URL: https://speka.media/visim-naipopulyarnisix-form-kiberzlociniv-u-interneti-pyweo9.
5. Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. *Юрист і Закон* (ТОВ «ЛІГА ЗАКОН»), № 45. 2022, 17 листопада. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606#.
6. Гончаренко І.Г. Кіберзагрози фінансового сектора в умовах війни. *Економіка та суспільство*. 2023. № 50/2023. С. 1–4. URL: http://surl.li/tjtmk.
7. Кібербезпека бізнесу в умовах нестабільності. 2022. URL: https://www.pwc.com/ ua/uk.
8. Кібербезпека в умовах війни: як встояти на інформаційному фронті. URL: https://pingvin.pro/gadgets/news-gadgets/kiberbezpeka-v-umovah-vijny-yak-vstoyaty-nainformaczijnomu-fronti.html.
9. Кібербезпека: Все що необхідно знати кожному користувачу мережі Інтернет. URL: https://www.ukraine-lifehacker.com/kiberbezpeka-vse-shcho-neobkhidnoznaty.
10. Некрасов В. Українці збагатили кібершахраїв на півмільярда: як не стати жертвою. URL: https://news.finance.ua/ua/news/-/419603/ukrayintsi-zbagatyly-kibershahrayiv-na-pivmilyarda-yak-ne-staty-zhertvoyu.
11. Озарслан С. Основні загрози та кіберризики, з якими зіткнуться фінансові послуги та банківські компанії у 2022 році. 2022. URL: http://surl.li/tjtdo.
12. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 5 липня 1994 р. *Відомості Верховної Ради України*. 1994. № 31. Ст. 9.
13. Проблеми українського суспільства: кіберзлочинність. 2023. URL: https://docplayer.net/71413983-Problemi-ukrayinskogo-suspilstva-kiberzlochinnist.html.
14. Скибун О.Ж. Кібергієна як складова формування цифрової держави. *Вісник НАДУ*. Серія «Державне управління». 2021. № 2. С. 39–46.
15. Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни: затверджено Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/lws/show/447/2021#Text.
16. Теплицький Б.Б. Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: дис. ... канд. юрид. наук: 12.00.09. Київ, 2021. 268 с.

17. Чаплінська Ю. Кіберкультура та кібербезпека в умовах війни: психологічний практикум: практичний посібник. Національна академія педагогічних наук України, Інститут соціальної та політичної психології. Київ, 2023. 80 с.
18. Яровенко Г.М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу. *Ефективна економіка*. № 7. URL: http://www.economy.nayka.com.ua/?op=1&z=6453.