УДК 340
DOI https://doi.org/10.24144/2788-6018.2024.06.113

МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФІЗИЧНИХ ОСІБ

Шевчук М.О.,
кандидат юридичних наук,
докторант кафедри конституційного,
адміністративного та фінансового права
Хмельницького університету управління та права
ім. Леоніда Юзькова

Шевчук М.О. Механізм забезпечення інформаційної безпеки фізичних осіб.

У статті розглядається механізм забезпечення інформаційної безпеки фізичних осіб. Акцентується увага на тому, що в законодавстві з'являється тенденція до презумпції інформаційної безпеки. Це є одним із правових засобів, що забезпечують інформаційну безпеку та захищають права власників інформації. Ця презумпція виконує кілька важливих функцій: забезпечує законність дій з інформацією, гарантує факт інформаційної безпеки, захищає права учасників інформаційних правовідносин, а також дозволяє оцінити значимість і цінність інформації. Користувачі інформації, щодо якої встановлюється презумпція інформаційної безпеки, оцінюють її значимість на основі закону або договору.

Дослідження механізму забезпечення інформаційної безпеки фізичних осіб вимагає врахування трьох ключових складових: технічні засоби захисту, правове регулювання та освітня складова. Кожен із цих елементів відіграє важливу роль у створенні надійної системи захисту персональних даних від загроз у цифровому середовищі. Досліджуються сучасні технічні засоби захисту, правове регулювання та роль освіти у підвищенні рівня обізнаності населення щодо інформаційної безпеки. Аналізується ефективність використання різних заходів захисту персональних даних, а також їх вплив на формування культури безпеки в суспільстві.

Ключовими висновками з дослідження є те, що впровадження сучасних технологічних рішень значно знижує ризики, пов'язані з кібератаками; наявність чітких правових норм і механізмів контролю забезпечує захист прав фізичних осіб на інформаційну безпеку; підвищення обізнаності громадян про основи інформаційної безпеки формує культуру безпеки в суспільстві.

Можливості для подальшого розвитку в цій сфері можуть містити наступне: впровадження нових методів захисту даних, враховуючи сучасні загрози в кіберпросторі; розширення досліджень у сфері правового регулювання для адаптації законодавства до змінних умов; покращення навчальних програм для різних груп населення з акцентом на практичні аспекти інформаційної безпеки.

Стаття також визначає невирішені питання в цій сфері та пропонує рекомендації щодо подальшого розвитку механізмів забезпечення інформаційної безпеки.

Ключові слова: інформаційна безпека, механізм забезпечення інформаційної безпеки фізичних осіб, технічні засоби захисту інформаційної безпеки фізичних осіб; правове регулювання інформаційної безпеки фізичних осіб.

Shevchuk M.O. The mechanism for ensuring information security of individuals.

The article examines the mechanism of ensuring information security of individuals. The author emphasizes that there is a tendency in legislation to presume information security. This is one of the legal means to ensure information security and protect the rights of information owners. This presumption performs several important functions: it ensures the legality of actions with information, guarantees the fact of information security, protects the rights of participants in information legal relations, and allows to assess the significance and value of information. Users of information subject to the presumption of information security assess its significance on the basis of law or contract.

The study of the mechanism for ensuring information security of individuals requires taking into account three key components: technical means of protection, legal regulation and educational component. Each of these elements plays an important role in creating a reliable system for protecting personal data from threats in the digital environment. Modern technical means of protection, legal regulation, and the role of education in raising public awareness of information security are studied. The effectiveness of various personal data protection measures and their impact on the formation of a security culture in society are analyzed.

The key conclusions of the study are that the introduction of modern technological solutions

significantly reduces the risks associated with cyberattacks; the existence of clear legal norms and control mechanisms ensures the protection of individuals' rights to information security; raising public awareness of the basics of information security creates a culture of security in society.

Opportunities for further development in this area may include the following: the introduction of new methods of data protection, taking into account modern threats in cyberspace; expanding research in the field of legal regulation to adapt legislation to changing conditions; improving training programs for various groups of the population with an emphasis on the practical aspects of information security.

The article also identifies unresolved issues in this area and offers recommendations for further development of information security mechanisms.

Key words: information security, the mechanism for ensuring the information security of individuals, technical means of protecting the information security of individuals; legal regulation of information security of individuals.

Постановка проблеми. В умовах стрімкого розвитку інформаційних технологій проблема інформаційної безпеки фізичних осіб набуває особливої актуальності. Відсутність належного захисту персональних даних може призвести до різноманітних загроз, таких як крадіжка особистих даних, фінансові збитки, а також психологічний тиск на жертв кіберзлочинців. Користувачі часто не усвідомлюють усіх ризиків, пов'язаних із їхньою діяльністю в Інтернеті, що робить їх вразливими до атак зловмисників. З огляду на це, важливо знайти ефективні рішення для забезпечення інформаційної безпеки, які б враховували як технічні, так і соціальні аспекти. Це завдання є надзвичайно важливим не лише для окремих фізичних осіб, але і для суспільства в цілому, оскільки зростання кількості інцидентів у сфері кібербезпеки негативно впливає на довіру до цифрових технологій і сервісів.

Метою даної статті є розробка механізму забезпечення інформаційної безпеки фізичних осіб, що охоплює як технічні, так і організаційні заходи. **Завданням** статті є визначення ключових компонентів цього механізму, їх взаємозв'язок та роль у забезпеченні загальної безпеки фізичних осіб.

Стан опрацюваннбя проблематики. Останні дослідження в галузі інформаційної безпеки акцентують увагу на різноманітних аспектах, що стосуються захисту персональних даних. Дослідження, проведене Коваленком В., підкреслює важливість системного підходу до захисту даних, зокрема в контексті використання соціальних мереж. Петрова І. у своїй статті акцентує увагу на правових аспектах захисту персональних даних, досліджуючи, як міжнародні норми можуть бути імплементовані в національне законодавство. Дослідження Кравченка О. зосереджується на новітніх технологіях захисту, зокрема на шифруванні та автентифікації. Ці публікації створюють основу для подальшого вивчення механізмів забезпечення інформаційної безпеки фізичних осіб.

Окремі проблеми цієї тематики досліджуються в працях: О.В. Арістової, О.А. Баранова, К.І. Бєлякова, В.М. Брижка, С.С. Єсімова, Р.А. Калюжного, М.В. Коваліва, О.В. Копана, В.К. Конаха, Б.А. Кормича, О.В. Коржа, О.В. Кохановської, О.В. Марущака, В.Г. Пилипчука, Н.А. Савінової, І.М. Шопіної, М.Я. Швеця і інших

Виклад основного матеріалу. Попри численні дослідження, існує кілька невирішених аспектів, які потребують подальшого вивчення. По-перше, недостатньо уваги приділено інтеграції технологічних, правових і освітніх компонентів в єдиний механізм забезпечення інформаційної безпеки фізичних осіб.

По-друге, не вистачає емпіричних досліджень, які б підтвердили ефективність різних підходів до навчання користувачів основам інформаційної безпеки. Нарешті, існує потреба у розробці рекомендацій щодо впровадження кращих практик захисту даних у повсякденне життя.

Метою даної статті є розробка механізму забезпечення інформаційної безпеки фізичних осіб, який би поєднував технічні, правові та освітні аспекти.

Завданням статті є визначення ключових компонентів цього механізму, їх взаємозв'язок, а також аналіз ефективності застосування різних заходів захисту персональних даних. Окрім того, стаття має на меті розкрити важливість підвищення рівня обізнаності населення щодо інформаційної безпеки та запропонувати рекомендації щодо впровадження кращих практик у повсякденному житті.

У сучасному світі інформаційні технології стали невід'ємною частиною повсякденного життя. З поширенням Інтернету та цифрових пристроїв зростає і кількість загроз, пов'язаних із інформаційною безпекою фізичних осіб. Проблема забезпечення інформаційної безпеки фізичних осіб вимагає комплексного підходу, адже вона безпосередньо впливає на приватність, конфіденційність даних і, в кінцевому підсумку, на загальний рівень безпеки в суспільстві. В умовах глобалізації, технологічного прогресу та розвитку кіберзлочинності питання захисту особистої інформації стає ще більш актуальним, оскільки зловмисники постійно шукають нові способи доступу до приватних даних.

Критерії інформаційної безпеки постійно ускладнюються, тому важливо не лише впрова-

джувати окремі заходи безпеки, а й формувати комплексну систему, що включає різноманітні інструменти та прийоми. Ці засоби можуть бути використані законодавцем або особами, що реалізують свої права для забезпечення інформаційної безпеки в різних соціальних відносинах. Засоби забезпечення безпеки поділяються на правові, організаційні, технічні та інші. Правові засоби складають сукупність прийомів, які закріплені у правових нормах для забезпечення інформаційної безпеки. Організаційні засоби містять прийоми організаційного характеру, що дозволяють підтримувати інформаційну безпеку в суспільних відносинах. Технічні та програмно-апаратні засоби передбачають використання певних технологій та програмного забезпечення для інформаційної безпеки, як, наприклад, електронний підпис.

Інформаційна безпека визначається не лише на рівні нормативно-правових актів, але й через технічні норми. Це включає впровадження технічних засобів для забезпечення інформаційної безпеки.

Загальні правові засоби інформаційної безпеки включають: законодавче визначення термінів, формування системи правового забезпечення, закріплення основних принципів, що стосуються системи заборон, зобов'язань, дозволів та інших правових інструментів. Система конкретних юридичних прийомів, що використовуються для забезпечення інформаційної безпеки, є певною сукупністю засобів і прийомів [13, с. 239].

В умовах інформаційного суспільства інформаційна безпека має стратегічне значення. З поширенням цифрових технологій, зокрема штучного інтелекту та платформних рішень, зростає ймовірність виникнення ризиків, пов'язаних із розповсюдженням недостовірної інформації. Принцип права на достовірну інформацію безпосередньо пов'язаний із забезпеченням інформаційної безпеки. Це виявляється у сукупності правових можливостей, закріплених за фізичними, юридичними особами та публічними утвореннями.

Деякі спеціальні суб'єкти наділяються цим правом, що є особливо важливим для фізичних осіб. Серед прав, що випливають з суб'єктивного права на захист інформації, можна виділити: право на оновлення, надання, уточнення та виправлення інформації, а також можливість використовувати достовірну інформацію. Встановлення пріоритетної форми або способу фіксації інформації є важливим для забезпечення інформаційної безпеки. Цей засіб включає закріплення відповідних форм і способів фіксації інформації на законодавчому рівні.

Законодавець визначає, що в разі сумнівів і суперечок пріоритет надається певній формі чи способу фіксації інформації. Визнання захищеної інформації може відбуватися шляхом офіційного електронного оприлюднення, зокрема публікацій. Цей підхід особливо важливий для правової інформації, де пріоритет мають офіційні джерела.

До пріоритетних способів фіксації інформації належать публічні реєстри, офіційні банки та бази даних. Офіційні, обов'язкові чи інші способи закріплення пріоритетності форм фіксації інформації грають важливу роль у забезпеченні інформаційної безпеки. Одним із правових засобів забезпечення інформаційної безпеки є публічне визнання, що можливе на основі виконання нормативних вимог про публічне визнання створеної інформації.

Публічна заява може бути сформульована на підставі вимог, що містяться в договорі, або шляхом прямого волевиявлення суб'єктів як гарантія забезпечення безпеки.

Визнання безпеки може відбуватися у різних формах, зокрема через заяви на виконання юридично значущих дій, розповсюдження інформації як безпечної, підписання угод та публікацію даних про це (що характерно для приватноправових відносин), а також через спеціальні свідоцтва про інформаційну безпеку.

Зі зростанням цифровізації, однією з форм визнання інформаційної безпеки є використання технологій блокчейн [3, с. 269]. Однією з ключових вимог до таких систем є незмінність інформації, що зберігається на платформі блокчейн, а також неможливість зміни без фіксації цього факту в системі [2, с. 42].

Будь-які зміни інформації фіксуються, що робить їх доступними для всіх користувачів платформи. Завдяки публічному відображенню всіх змін, встановлюється важлива гарантія забезпечення захисту. Такі форми визнання інформаційної безпеки є перспективними і активно розвиваються в бізнес-процесах, а також у сфері публічного управління, де забезпечення довіри до цифрового середовища та використовуваних технологій є критично важливим.

Перевірки також є важливим засобом забезпечення інформаційної безпеки. Перевірка проводиться в рамках надання адміністративних послуг. Наприклад, Міністерство юстиції України під час ведення державного реєстру громадських об'єднань перевіряє повноту поданих документів. У правовому регулюванні спостерігається тенденція закріплення перевірки інформації в усіх офіційних інформаційних потоках.

Перевірка безпеки здійснюється шляхом запиту додаткових відомостей або документів, що підтверджують достовірність інформації. Для цього можуть використовуватися звернення та запити відповідно до установленого порядку. Можуть бути встановлені спеціальні терміни та вимоги до змісту відповідей на запити.

Перевірку інформаційної безпеки можуть проводити як учасники інформаційних процесів, так і незалежні зовнішні суб'єкти. Наприклад, під час аудиторських перевірок застосовуються організаційні заходи, що включають зіставлення, порівняння, аналіз та інші методи, а також технічні та програмно-апаратні засоби [4, с. 26].

Технології штучного інтелекту активно використовуються для перевірки ідентифікації недостовірної інформації на рівні повідомлень, відео, акаунтів у мережі Інтернет та сайтів.

Перевірка безпеки розглядається як частина інформаційних процесів і адміністративних процедур, проте може бути й самостійною процедурою. Держава повинна розробити систему прийомів, що реалізує цю самостійну адміністративну процедуру.

У законодавстві з'являється тенденція до презумпції інформаційної безпеки. Це є одним із правових засобів, що забезпечують інформаційну безпеку та захищають права власників інформації. Презумпція безпеки означає, що власник інформації при наданні або розповсюдженні інформації третім особам має гарантію, що йому не потрібно виконувати додаткові дії для доведення факту безпеки. Це спрощує обіг інформації та знижує витрати на окремі операції [8, с. 82]. Для користувачів інформації, які отримують інформацію від власника, виникає гарантія, що вони використовують достовірну інформацію. Презумпція інформаційної безпеки свідчить, що інформація визнається безпечною, допоки не буде доведено зворотне.

Ця презумпція виконує кілька важливих функцій: забезпечує законність дій з інформацією, гарантує факт інформаційної безпеки, захищає права учасників інформаційних правовідносин, а також дозволяє оцінити значимість і цінність інформації. Користувачі інформації, щодо якої встановлюється презумпція інформаційної безпеки, оцінюють її значимість на основі закону або договору. Вони вище оцінюють інформацію, що охороняється презумпцією інформаційної безпеки, ніж іншу інформацію. Це стає важливим інструментом у правових відносинах, а також для захисту прав фізичних і юридичних осіб у всіх інформаційних процесах.

Інформаційна безпека є основоположною умовою для діяльності держави, а також бізнесу та кожного громадянина. У сучасному світі, насиченому інформацією, важливо не лише мати доступ до достовірних даних, але й мати впевненість у безпеці цієї інформації [12, с. 22].

Узагальнюючи, інформаційна безпека включає систему різних засобів, що забезпечують правовий захист, організаційні рішення та технічні інструменти. Зростання цифрових технологій, розвиток штучного інтелекту і впровадження нових форм визнання інформаційної безпеки є важливими кроками на шляху до ефективного забезпечення безпеки інформації у всіх сферах суспільства.

Дослідження механізму забезпечення інформаційної безпеки фізичних осіб вимагає врахування трьох ключових складових: технічні засоби захисту, правове регулювання та освітня складова. Кожен із цих елементів відіграє важливу роль у створенні надійної системи захисту персональних даних від загроз у цифровому середовищі. Їхня інтеграція та ефективне функціонування дозволяють не лише захистити інформацію від несанкціонованого доступу, а й забезпечити відповідальне та обізнане використання цифрових технологій.

1. Технічні засоби захисту

Технічні заходи захисту – це базова складова інформаційної безпеки, яка забезпечує фізичним особам захист від кібератак та інших загроз у цифровому середовищі. До основних засобів відносяться: антивірусне програмне забезпечення, фаєрволи, шифрування даних, резервне копіювання, багатофакторна автентифікація, а також регулярне оновлення програмного забезпечення.

Основні технічні заходи:

а) Антивірусне програмне забезпечення. Антивіруси сканують файли та системи на наявність шкідливого програмного забезпечення, яке може викрасти або пошкодити дані. Згідно з останніми дослідженнями, своєчасне оновлення антивірусів підвищує ефективність захисту на 30-40%, що дозволяє значно знизити ризики зараження системи вірусами або шкідливими програмами.

б) Шифрування даних. Шифрування перетворює дані на недоступні для сторонніх осіб без відповідного ключа доступу. Використання передових алгоритмів шифрування дозволяє запобігти крадіжці персональних даних у 90% випадків. Це стає особливо важливим у випадках збереження конфіденційної інформації, як-от фінансові або медичні дані.

в) Регулярне оновлення програмного забезпечення. Виробники програмного забезпечення постійно вдосконалюють свої продукти, виправляючи вразливості, які можуть бути використані кіберзлочинцями. За даними експертів, пропуск оновлень збільшує ризик вразливостей до атак на 50%. Таким чином, регулярні оновлення ОС, браузерів і додатків є обов'язковою умовою підтримання безпеки.

г) Багатофакторна автентифікація (МФА). Впровадження МФА значно підвищує рівень безпеки, оскільки для доступу до системи або даних користувач повинен підтвердити свою особу не лише через пароль, а й через додатковий фактор, наприклад, SMS-код або біометрію. Це

ефективно знижує ризик злому облікових записів, навіть якщо пароль був скомпрометований.

д) Фаєрволи та системи захисту від вторгнень (IPS/IDS). Важливими елементами є також фаєрволи, які контролюють вхідний і вихідний трафік, а також системи виявлення та запобігання атак, що дозволяють вчасно реагувати на потенційні загрози [6, с. 52].

2. Правове регулювання

Правове регулювання захисту персональних даних є фундаментом для забезпечення прав фізичних осіб на конфіденційність та безпеку їхньої інформації. Важливим елементом цієї складової є наявність законодавчих актів, що регламентують обробку та зберігання даних, а також передбачають відповідальність за порушення [9, с. 32]

Основні законодавчі положення: Законодавство про захист персональних даних**.** В Україні основним документом, що регулює цей процес, є Закон «Про захист персональних даних» [5], який закріплює права фізичних осіб на конфіденційність їхніх даних, а також обов'язки для організацій, що їх обробляють. Це включає: обов'язок зберігати дані лише протягом необхідного часу; заборону передачі даних третім сторонам без дозволу;вимоги до організацій щодо запровадження технічних заходів захисту.

GDPR (Загальний регламент про захист даних). На міжнародному рівні важливим стандартом є GDPR, який регулює захист даних у країнах Європейського Союзу. Він встановлює суворі вимоги до захисту даних і значні штрафи за їх порушення. Українські компанії, що співпрацюють із ЄС, також повинні дотримуватися цього регламенту [14].

Механізми контролю та аудиту. Регулювання передбачає створення спеціальних державних і приватних органів, які займаються моніторингом дотримання законодавства у сфері інформаційної безпеки. Це дозволяє запобігти неправомірному використанню особистої інформації і своєчасно виявляти порушення.

3. Освіта та підвищення обізнаності

Технічні засоби і правові механізми ефективні лише в поєднанні з високим рівнем обізнаності громадян щодо безпечного використання Інтернету та збереження власних даних. Цифрова грамотність – це ключ до ефективної інформаційної безпеки [10, с. 57].

Основні заходи для підвищення обізнаності:

Тренінги та семінари. Проведення навчальних заходів для широких верств населення є одним із важливих кроків до підвищення їхньої обізнаності про загрози в мережі та методи захисту. Наприклад, на таких тренінгах користувачів навчають: Як розпізнати фішингові атаки. Як захищати свої облікові записи паролями та багатофакторною автентифікацією. Які налаштування конфіденційності використовувати в соціальних мережах [1, с. 102].

Інформаційні кампанії. Запуск національних кампаній з популяризації захисту даних та безпечного користування цифровими технологіями може зменшити кількість успішних кібератак на 20-30%. Такі кампанії можуть включати рекламні оголошення, соціальні мережі та освітні платформи.

Освітні програми в навчальних закладах. Важливо інтегрувати уроки інформаційної безпеки до шкільної та університетської освіти, щоб молоді люди з раннього віку знали про ризики в цифровому просторі та могли їх уникати.

Забезпечення інформаційної безпеки фізичних осіб – це комплексний процес, який передбачає тісну взаємодію технічних засобів, правових механізмів та освітніх заходів. Інтеграція цих компонентів у єдиний механізм суттєво підвищує рівень захисту персональних даних, знижуючи ризики несанкціонованого доступу та неправомірного використання інформації.

Правове регулювання охоплює національні закони та міжнародні норми, які захищають права фізичних осіб у сфері обробки персональних даних. Наприклад, Загальний регламент про захист даних (GDPR) Європейського Союзу встановлює жорсткі вимоги до обробки персональних даних і забезпечує права користувачів. В Україні питання захисту персональних даних регулюється Законом «Про захист персональних даних», що є важливим кроком у напрямку забезпечення інформаційної безпеки.

Освіта громадян також є важливим елементом механізму забезпечення інформаційної безпеки. Підвищення рівня обізнаності населення про основи інформаційної безпеки, правила безпечного користування Інтернетом та соціальними мережами допомагає зменшити ризики, пов'язані з кіберзлочинністю. Навчання людей основам захисту своїх даних, а також використання безпечних практик у повсякденному житті є невід'ємною частиною системи інформаційної безпеки.

Дослідження підтвердило, що забезпечення інформаційної безпеки фізичних осіб є складним і багатогранним процесом, який вимагає комплексного підходу. Технічні, правові та освітні аспекти повинні взаємодіяти, щоб створити ефективну систему захисту персональних даних [7, с. 12].

Ключовими висновками з дослідження є: впровадження сучасних технологічних рішень значно знижує ризики, пов'язані з кібератаками; наявність чітких правових норм і механізмів контролю забезпечує захист прав фізичних осіб на інформаційну безпеку; підвищення обізнаності громадян про основи інформаційної безпеки формує культуру безпеки в суспільстві.

Перспективи подальшого розвитку в даному напрямі можуть включати: розробку нових технологій для захисту даних, враховуючи сучасні загрози в кіберпросторі; поглиблення досліджень в сфері правового регулювання, щоб адаптувати законодавство до змінюваних умов; вдосконалення програм навчання для різних груп населення, з акцентом на практичні аспекти інформаційної безпеки [11, с. 100].

Висновки. Таким чином, інформаційна безпека фізичних осіб залишається важливою темою для дослідження та практичної реалізації, яка вимагатиме постійного удосконалення механізмів захисту в умовах швидко змінюваного технологічного середовища.

Висновки з проведеного дослідження свідчать про те, що забезпечення інформаційної безпеки фізичних осіб потребує комплексного підходу, що поєднує технологічні, правові та освітні аспекти. Розроблений механізм, що включає в себе ці три компоненти, може суттєво підвищити рівень захисту персональних даних та знизити ризики, пов'язані з інформаційною безпекою. Перспективи подальшого розвитку в цьому напрямі включають вдосконалення існуючих технологій захисту, інтеграцію новітніх правових норм, а також активізацію просвітницької діяльності серед населення для формування культури безпеки в інформаційному середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Арістова І.В., Баранов О.А., Дзьобань О.П. та ін. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія. Київ: КВІЦ, 2019. 344 с.
2. Грищенко, А. Проблеми інформаційної безпеки в Україні: шляхи їх подолання. *Журнал українського права*, 2023. № 11(5). С. 38–50.
3. Гурова А., Кірпачова М. Правові засади застосування блокчейну в космічній діяльності: особливості регулювання технології на національному, регіональному та міжнародному рівнях. *Підприємництво, господарство і право.* 2021. № 1. С. 265–275.
4. Єсімов С.С. Використання інформаційних технологій як предмет адміністративно-правового регулювання. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки.* 2015. № 827. С. 24–29.
5. Про захист персональних даних: Закон України. *Відомості Верховної Ради України*. 2010. № 30. Ст. 236.
6. Коваленко В. Соціальні мережі і питання захисту персональних даних: нові виклики та загрози. *Журнал інформаційної безпеки*. 2022. № 3(1). С. 45–56.
7. Ковалів М.В., Єсімов С.С., Кравчук С.М. Теоретичні засади правового регулювання систем штучного інтелекту щодо ідентифікації особи у контексті діяльності органів виконавчої влади. *Соціально-правові студії.* 2020. Випуск 2 (8). С. 8–15.
8. Кравченко О. Новітні технології захисту даних: аналіз та перспективи. *Наукові записки Інституту кібернетики*. № 15(2), 2022. С. 75–88.
9. Петрова І. Правове регулювання захисту персональних даних в Україні: сучасний стан і перспективи. *Право та інформація*. № 2(4), 2021. С. 28–37.
10. Тарасенко Ю. Освіта в сфері інформаційної безпеки: виклики та можливості. *Актуальні проблеми інформаційної безпеки*. 2023. № 4(3). С. 54–64.
11. Хмельницький В. Актуальні питання забезпечення інформаційної безпеки громадян в епоху цифровізації. *Вісник Національної академії державного управління*. 2022. № 12(2). С. 89–101.
12. Шаповалов Д. Кібербезпека: нові тренди та технології. *Міжнародний журнал кібербезпеки*, 2022. № 6(1). С. 14–25.
13. Ярема О.Г. Система правових засобів забезпечення інформаційної безпеки. *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2022. С. 237–242.
14. GDPR (General Data Protection Regulation). (2016). *Official Journal of the European Union*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679.