УДК 004.738:004.056
DOI: https://doi.org/10.32782/IT/2026-2-10

Олександр ЗАДЕРЕЙКО
кандидат технічних наук, доцент, доцент кафедри штучного інтелекту та математичного моделювання, Національний університет «Одеська юридична академія», вул. Рішельєвська, 28, м. Одеса, Україна, 650011
ORCID: *0000-0003-0497-9861*
Scopus-Author ID: *57196005917*

Світлана ЄЛЕНИЧ
головний бібліограф наукової бібліотеки,
Національний університет «Одеська юридична академія», вул. Рішельєвська, 28, м. Одеса, Україна, 650011
ORCID: *0000-0003-4999-3034*

Володимир ГУРА
кандидат технічних наук, доцент кафедри штучного інтелекту та математичного моделювання, Національний університет «Одеська юридична академія», вул. Рішельєвська, 28, м. Одеса, Україна, 650011
ORCID: *0009-0001-2166-5410*

Олена ТРОФИМЕНКО
кандидат технічних наук, доцент, доцент кафедри програмної інженерії, Національний університет «Одеська юридична академія», вул. Рішельєвська 28, м. Одеса, Україна, 650011
ORCID: *0000-0001-7626-0886*
Scopus-Author ID: *57189319394*

Оксана ГАЙДАЄНКО
кандидат технічних наук, доцент, доцент кафедри інформаційних управляючих систем та технологій, Національний університет кораблебудування імені адмірала Макарова, проспект Героїв України, 9, м. Миколаїв, Україна, 54007
ORCID: *0000-0002-6614-5443*
Scopus-Author ID: *59243568400*

Лідія МАКАРОВА
кандидат технічних наук, доцент, доцент кафедри програмного забезпечення автоматизованих систем, Національний університет кораблебудування імені адмірала Макарова, проспект Героїв України, 9, м. Миколаїв, Україна, 54007
ORCID: *0000-0003-2903-3001*
Scopus ID: 57200142648

Бібліографічний опис статті: Задерейко, О., Єленич, С., Гура, В., Трофименко, О., Гайдаєнко О., Макарова Л. (2026). Аналіз стану захисту персональних даних в умовах взаємодії суб'єктів у мережевому середовищі. *Information Technology: Computer Science, Software Engineering and Cyber Security*, doi: https://doi.org/10.32782/IT/2026-2-10

АНАЛІЗ СТАНУ ЗАХИЩЕНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ВЗАЄМОДІЇ СУБ'ЄКТІВ У МЕРЕЖЕВОМУ СЕРЕДОВИЩІ

У статті розглядаються особливості формування загроз витоку персональних даних в умовах інтенсивної взаємодії суб'єктів у мережевому середовищі. Особлива увага приділяється взаємодії суб'єктів обробки персональних даних, зокрема користувачів, операторів та третіх осіб, а також потенційним ризикам, що виникають під час транскордонної передачі даних у мережевому середовищі.

Метою статті *є аналіз і систематизація персональних даних що можуть бути використані для електронної ідентифікації користувачів та організація їх захисту від потенційних витоків з комунікаційних пристроїв у мережевому середовищі.*

Методологія. *Проведено порівняльний аналіз захищеності персональних даних. Використано метод систематизації даних для дослідження загальної схеми верифікації користувачів у мережевому середовищі. Описано оптимальний підхід, що дозволяє забезпечити захист персональних даних на пристрої комунікації користувача від потенційних витоків у мережевому середовищі.*

Наукова новизна. *Розглядаються основні особливості формування загроз витоку персональних даних в умовах розподіленого мережевого середовища, аналізуються сучасні підходи до їх захисту з точки зору чинного законодавства України та Європейського Союзу, а також досліджуються підходи щодо забезпечення їх захисту на рівні архітектури інформаційно-комунікаційних систем.*

Висновки. *З'ясовано, що ідентифікатори у мережевому середовищі невід'ємна складова системи ідентифікації персональних даних особи та її мережевого профілю. А також були виокремлені в окрему категорію технічні ідентифікатори комунікаційних пристроїв, які у поєднані з будь-якими персональними даними або конфіденційною/публічною інформацією дають змогу ідентифікувати особу у мережевому середовищі. Тому всі персональні дані, що можуть бути використані системами ідентифікації громадян потребують посиленого та надійного захисту.*

Ключові слова: *комунікаційні пристрої користувачів, ідентифікація особи у мережевому середовищі, персональні дані суб'єктів мережевого середовища, потенційні витоки персональних даних, захист персональних даних, обробка персональних даних, GDPR.*

Olexander ZADEREYKO
Candidate of Technical Sciences, Associate Professor at the Department of the Artificial Intelligence and Mathematical Modeling, National University "Odesa Law Academy", 28, Richelyevska St., Odessa, Ukraine, 650011, zadereyko@onua.edu.ua
ORCID: *0000-0003-0497-9861*
Scopus-Author ID: *57196005917*

Svitlana YELENYCH
Chief Bibliographer of the Scientific Library, National University "Odessa Law Academy", 28, Richelyevska St., Odesa, Ukraine, 650011, o.yelenych@onua.edu.ua
ORCID: *0000-0003-4999-3034*

Volodymyr HURA
Candidate of Technical Sciences, Associate Professor at the Department of the Artificial Intelligence and Mathematical Modeling, National University "Odesa Law Academy", 28, Richelyevska St., Odesa, Ukraine, 650011, hura@onua.edu.ua
ORCID: *0009-0001-2166-5410*

Olena TROFYMENKO
Candidate of Technical Sciences, Associate Professor at the Department of the Software Engineering, National University "Odessa Law Academy", 28, Richelyevska St., Odesa, Ukraine, 650011, trofymenko@onua.edu.ua
ORCID: *0000-0001-7626-0886*
Scopus-Author ID: *57189319394*

Oksana HAIDAIENKO
Candidate of Technical Sciences, Associate Professor at the Department of Information Control Systems and Technology, Admiral Makarov National University of Shipbuilding, 9, Heroes of Ukraine Ave., Mykolaiv, Ukraine, 54007, oksana.gaidaienko@nuos.edu.ua
ORCID: *0000-0002-6614-5443*
Scopus-Author ID: *59243568400*

Lidiia MAKAROVA
Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Software of Automated Systems, Admiral Makarov National University of Shipbuilding, 9, Heroes of Ukraine Ave., Mykolaiv, Ukraine, 54007, lidiia.makarova@nuos.edu.ua
ORCID: *0000-0003-2903-3001*
Scopus-Author ID: *57200142648*

To cite this article: Zadereyko, O., Yelenych, S., Hura, V., Trofymenko, O., Haidaienko, O., Makarova, L. (2026). Analiz stanu zakhystu personalnykh danykh v umovakh vzaiemodii sub'iektiv u merezhevomu seredovyshchi [Analysis of the state of personal data protection in the context of interaction between entities in network environment]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, doi: https://doi.org/10.32782/IT/2026-2-10

ANALYSIS OF THE STATE OF PERSONAL DATA PROTECTION IN THE CONTEXT OF INTERACTION BETWEEN ENTITIES IN NETWORK ENVIRONMENT

The aim of the article is to analyze and categorize the personal data that can be used for the electronic identification of users and to organize measures to protect such data from potential leaks from communication devices in the digital environment.

The methodology. *A comparative analysis of personal data security was conducted. A data systematization method was used to study the general scheme of user verification in a network environment. An optimal approach is described that allows protecting personal data on the user's communication device from potential leaks in a network environment.*

The scientific novelty. *This paper examines the key characteristics of the emergence of personal data breach risks in a distributed digital environment, analyzes current approaches to protecting such data in light of applicable Ukrainian and European Union legislation, and explores methods for ensuring their protection at the level of information and communication systems architecture.*

The conclusions. *It has been established that identifiers in a network environment are an integral part of the system for identifying an individual's personal data and their digital profile. In addition, technical identifiers of communication devices were classified into a separate category; when combined with any personal data or confidential/public information, these identifiers make it possible to identify an individual in the digital environment. Therefore, all personal data that can be used by citizen identification systems requires enhanced and reliable protection.*

Key words: *users' communication devices, identity verification in the digital environment, personal data of digital environment users, potential personal data breaches, personal data protection, personal data processing, GDPR.*

Постановка проблеми. В умовах повсюдної цифровізації комунікаційного середовища персональні дані користувачів стають цінним ресурсом, який забезпечує їх ідентифікацію та взаємодію з електронними сервісами та платформами різного призначення. Попри наявність нормативно-правових механізмів регулювання питань захисту персональних даних, серед яких Закон України «Про захист персональних даних», Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Convention 108), General Data Protection Regulation (GDPR), спостерігається стійке збільшення інцидентів, пов'язаних із витоком, несанкціонованим доступом та вторинним використанням персональних даних. Це зумовлено низкою факторів, а саме: складністю архітектури інформаційно-комунікаційних систем, неузгодженістю між суб'єктами баз персональних даних та операторами комунікаційного середовища, фактично прихованим збором персональних даних комунікаційних пристроїв користувачів, а також відсутністю засобів належного захисту персональних даних від витоків у мережевому середовищі.

Особливої актуальності набуває проблема прихованої передачі даних операційними системами Android та iOS, де фонові процеси обміну даними можуть призвести до збору конфіденційної інформації користувача. Наявні підходи до аналізу захищеності часто орієнтовані на окремі компоненти операційних систем (ОС) без забезпечення цілісного уявлення про масштаби витоків персональних даних користувачів. Тому актуальною є потреба розробки комплексного підходу, який дозволить враховувати взаємозв'язки між технічними, організаційними й поведінковими аспектами виявлення прихованих загроз, та формування обґрунтованих заходів щодо їх мінімізації. Рішення цієї проблеми потребує аналізу систем збору персональних даних та оцінки ризиків їх витоку з урахуванням сучасних комунікаційних пристроїв.

Аналіз останніх досліджень та публікацій. В період активної цифровізації суспільних та економічних процесів проблема захисту персональних даних набуває системного характеру та стає важливим елементом забезпечення інформаційної безпеки людини і суспільства. Зростання кількості цифрових сервісів, розвиток хмарних технологій, розповсюдження мобільних платформ та інтеграція інтелектуальних систем призводить до накопичення обсягів оброблених даних й ускладнення структури взаємодії суб'єктів мережевого простору. Це, в свою чергу, формує загрози витоків персональних даних, обумовлені як технічними, так і організаційними факторами.

Захист персональних даних базується на сукупності правових, організаційних і програмно-апаратних засобів, направлених на забезпечення конфіденційності, цілісності та доступності приватної інформації суб'єктів мережевого середовища. В Україні забезпечення конфіденційності персональних даних ґрунтується на дотриманні вимог чинного законодавства, європейських і міжнародних стандартів, ратифікованих Україною, стандартів інформаційної безпеки, нормативних документів з питань технічного та операційного захисту інформації, інших галузевих нормативно-правових актів. Питання отримання, поширення, оброблення інформації про фізичних осіб та її захист регулюють закони України «Про інформацію», «Про захист персональних даних», «Про доступ до публічної інформації». Поняття «персональні дані» охоплює відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути особисто ідентифікована (Закони України № 2657-XII, 1992; № 2297-VI, 2010). Визначення того, наскільки власник персональних даних піддається ідентифікації залежить від поточних обставин. Зазначається, що «доступ до конфіденційної інформації обмежується фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов» (Закон України № 2939-VI, 2011). За відсутності згоди від фізичної особи персональних даних, інформація може бути поширена лише у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Перелік персональних даних, які є конфіденційною інформацією про фізичну особу, зазначено у статті 11 Закону України «Про інформацію», а саме: дані про освіту, сімейний стан, релігійні переконання, національність, стан здоров'я, адреса, дата і місце народження (Закон України № 2657-XII, 1992). Цей перелік даних про особу не є вичерпним. До конфіденційної інформації відносять відомості про майновий стан фізичної особи та інші її персональні дані (Рішення КСУ № 5-зп, 1997), а також інформацію про особисте і сімейне життя (Рішення КСУ № 2-рп/2012, 2012). Слід підкреслити, що список персональних даних, за якими можна ідентифікувати особу, містить доволі значний обсяг різної інформації – від відомостей про публічну діяльність до обставин приватного життя і подробиць в особистих стосунках.

Відповідно до пункту 8 статті 6 Закону України «Про захист персональних даних» «персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися» (Закон України № 2297-VI, 2010). В процесі взаємодії системи цифрової ідентифікації особи (дисконтна картка або банківська карта) з масивом даних (наприклад, чек на купівлю товарів), виникає можливість її ідентифікувати: якщо збирати, накопичувати і додавати до мережевого профілю особи її IP-адресу, версію ОС пристрою, геолокацію та інші дані, то це дозволяє виділити із кола клієнтів реальну особу, що автоматично накладає на власника бази даних зобов'язання щодо захисту цієї інформації від викрадення і розповсюдження.

У міжнародній практиці основним нормативно-правовим документом є GDPR. Законодавство України у сфері захисту персональних даних послідовно інтегрує принципи обробки персональних даних встановлені GDPR, який зобов'язує операторів даних впроваджувати багаторівневі системи захисту. Одними з фундаментальних принципів щодо оброблення персональних даних є принцип «захисту даних за призначенням» і принцип «захисту даних за замовчуванням» (GDPR, 2018).

Варто обґрунтовувати, з якою метою обробляються персональні дані, та встановлювати чітку межу між використанням даних для аналізу та їх використанням для впливу на людину. У GDPR зазначається, що результат опрацювання даних для статистичних цілей є агрегованими даними, тобто є не персональними даними. При цьому результат або персональні дані не використовують задля підтримки заходів або рішень щодо будь-якої визначеної фізичної особи (GDPR, 2018). Якщо зібрані відомості допомагають фінансовій установі підтвердити, що молодь частіше бере кредит, –

це статистика. Якщо ці самі дані стали причиною відмови конкретному юнаку в одержанні кредиту – це вже обробка персональних даних. Статистична ціль перетворює «приватне» на «суспільне» та гарантує, що персональні дані працюють на розвиток науки, економіки чи медицини. Така мета вимагає зовсім іншого рівня згоди та захисту. При цьому виключається ризик маніпуляції або переслідувань на основі персональних характеристик осіб.

За умов повсякденного зростання цифрової взаємодії суб'єктів, бази даних стали одним із найцінніших ресурсів, а їх формування, накопичення, обробка та використання стали основою для цифрової сфери суспільства і держави. Однак, з розширенням доступу до мережевого простору зростає і загроза порушення права на приватність майже у більшості сфер життєдіяльності громадян. Кожен крок громадянина у мережевому середовищі формує цифровий відбиток, який може бути використаний для створення детального профілю його особистості (Zadereyko et al., 2022). Отже, реалізація громадянами України своїх прав та обов'язків у мережевому просторі зумовлює виникнення «мережевого громадянства». Дієздатність мережевого громадянства країни напряму залежить від заходів посиленого захисту та безпечного розміщення електронних систем державних реєстрів, баз персональних даних та пов'язаних з ними резервних копій на серверах як на території України та за її межами (Задерейко та ін., 2025). Даний підхід потребує обліку ризиків для прав і свобод суб'єктів даних на всіх етапах обробки даних.

У мережевому середовищі під час зберігання, документообігу, обміну та передачі захист персональних даних набуває міждисциплінарного характеру, оскільки об'єднує методи інформаційної безпеки, права та управління ризиками.

Задля захисту персональних даних і конфіденційної інформації застосовують:

- засоби контролю, які обмежують доступ до баз і реєстрів даних згідно з регламентом систем цифрової ідентифікації та контролю доступу громадян на території України та за її межами (Закони України № 2155 VIII, 2017; № 1150, 2023);
- технології криптографічного захисту, які забезпечують цілісність і конфіденційність даних при транскордонній передачі та збереженні даних (Spevakov et al., 2020; Bogdanov et al., 2023);
- технології, які дозволяють знизити вірогідність небажаної ідентифікації користувачів за рахунок заборони прихованого збору даних (Dalal et al., 2026);
- технології виявлення несанкціонованих витоків даних (Nayak & Ojha, 2019; Saqib et al., 2025).

Несанкціоновані витоки персональних даних суб'єктів у мережевому середовищі є одним із поширених типом інцидентів у сфері інформаційної безпеки. Причини витоку даних можуть бути кваліфіковані факторами технічного, організаційного та людського походження. До технічних факторів відносять: вразливість програмно-апаратного забезпечення, помилки конфігурації систем захисту та незахищеність каналів передачі даних. Організаційні фактори містять відсутність або невідповідність регламенту захисту даних. Людський фактор переважно пов'язаний з діями користувачів та зловмисними намірами розробників програмного забезпечення.

Результати розглянутих досліджень обумовлюють потребу проведення ґрунтовного аналізу та виокремлення технічних даних, які у поєднанні з іншими персональними даними можуть призвести до однозначної ідентифікації суб'єкта у мережевому середовищі та розробити практичні рекомендації, які дозволять запобігти їх несанкціонованим витокам даних.

Метою статті є аналіз і систематизація персональних даних, які можуть бути використані для електронної ідентифікації користувачів, та організація їх захисту від потенційних витоків з комунікаційних пристроїв у мережевому середовищі.

Результати дослідження. Мережевий простір характеризується складністю структури взаємодії суб'єктів, а саме користувачів, операторів даних, постачальників послуг та третіх сторін. У межах цієї взаємодії формуються різні потоки даних, по яким здійснюється: передача даних між користувачем та сервісом; обмін даними між сервісами; транскордонна передача інформації. Розподілені системи оброблення даних відіграють важливу роль при передачі інформації між суб'єктами. Це збільшує поверхню атаки та ускладнює контроль над потоками даних. Разом з цим, у деяких випадках виявити, хто є контролером даних важко, особливо у децентралізованих системах, як-от блокчейн.

Постійна взаємодія особи з різноманітними електронними сервісами невпинно генерує стійкі набори персональних даних, які відображають її активність у мережевому середовищі. Ключова загроза криється у неперервному накопиченні таких даних про конкретну особу:

їх ретельне опрацювання відкриває можливість виявляти неочевидні поведінкові закономірності та формувати предиктивні моделі її поведінки. За умови цілеспрямованого і систематичного застосування такий аналіз здатний слугувати інструментом маніпуляції настановами широкої інтернет-аудиторії.

В останні роки виникла практика видалення частини інформації при передачі персональних даних у мережеве середовище. Це робиться для того, щоб зберегти конфіденційність або обмежити доступ до даних так, щоб їх можна було обробляти як «неперсональні дані». Така практика суттєво спрощує дотримання чинного законодавства, яке зазвичай вимагає щонайменшого рівня захисту для «деперсоналізованих даних» (Quach et al., 2022). Технології розпізнавання образів та аналізу великих даних дозволяють проводити повторну ідентифікацію суб'єктів базуючись на зібраних масивах даних. З огляду на стрімкий розвиток технологій ідентифікації, дані, які наразі вважаються анонімними, можуть втратити цей статус у майбутньому.

Технології спостереження за людиною вбудовані майже у кожний комунікаційний пристрій. Будь-то розумний годинник, фітнес-трекери активності, мережеве програмне забезпечення, застосунки, давачі та об'єкти «розумного дому» або мережі Інтернету речей перетворюють приватне життя особи на масив даних, доступних для аналізу. Завдяки вбудованим розробниками властивостям ці пристрої забезпечують автоматичну передачу даних операторам чи іншим суб'єктам, зокрема державним органам, медичним установам, роботодавцям, страховикам або комунальним підприємствам, без залучення кінцевого власника чи користувача. Втім, вилучення значущих ознак із набору даних може виявитись неефективним механізмом захисту конфіденційності особи, оскільки дозволяє подекуди відновити цю інформацію.

Цифрові відносини між державою та громадянами базуються на системі електронної ідентифікації фізичних осіб. Процес ідентифікації відбувається на основі унікальних даних фізичної особи (біометричні дані, логіни/паролі, електронні посвідчення особи, цифровий підпис), які є основою для формування «мережевого профілю» та забезпечують доступ до електронних послуг, комерції та соціальних мереж. Комунікаційні системи контролю доступу, зокрема електронна ідентифікація, автентифікація, біометрична верифікація, система BankID, електронний портал «Дія», стають найважливішими факторами визначення порядку здійснення захисту персональних даних суб'єктів.

Аналіз актуальних публікацій надав змогу здійснити систематизацію даних, які прямо або у поєднанні між собою дозволяють ідентифікувати особу у мережевому середовищі. До системи ідентифікації особи входять:

- персональні дані ідентифікованої особи – відомості про особу (прізвище, ім'я та по батькові, дата та місце народження, адреса, РНОКПП), особливо чутливі дані (зокрема, охоплюють відомості зі сфери фінансів, податків, здоров'я, нерухомості, релігійного переконання, етнічного походження) та біометричні дані;
- конфіденційна інформація ідентифікованої особи – дані про особисті та сімейні відносини, які стають відомими для широкого загалу при викрадені та можуть бути розміщені, щоб завдати шкоди репутації людини;
- публічна інформація ідентифікованої особи – відомості, які людина самостійно розміщує у мережевому середовищі або дані, які можуть бути отримані із загальнодоступних джерел (електронних реєстрів, баз персональних даних, сайтів, інших цифрових ресурсів);
- унікальні технічні ідентифікатори – дані мережевого профілю особи та її комунікаційного пристрою, які формуються внаслідок мережевої взаємодії комунікації особи у мережевому просторі.

У мережевому середовищі технічні ідентифікатори будь-якого комунікаційного пристрою автоматично генеруються та збираються електронними сервісами в процесі взаємодії його операційної системи та застосунків з цифровим простором (Zadereyko et al., 2022). Саме ці дані формують унікальний цифровий відбиток комунікаційного пристрою користувача у мережевому просторі.

Використання відвіданих особою URL та IP-адреса особи перетворює ці технічні ідентифікатори на об'єкт захисту від потенційних зловмисників, оскільки вище наведені складові дозволяють співвіднести особу у мережевому середовищі з реальною людиною. Згідно з GDPR фізичні особи можуть бути пов'язані з онлайн-ідентифікаторами за допомогою їхніх пристроїв, застосунків, інструментів чи протоколів, зокрема IP-адрес, ідентифікаторів cookie або інших ідентифікаторів. Це може залишити підказки, які, особливо в поєднанні з унікальними ідентифікаторами та іншою інформацією, отриманою із серверів, можна використати для створення профілів фізичних

осіб та їхньої ідентифікації (GDPR, 2018). Як статичні, так і динамічні IP-адреси відносять до категорії персональних даних, оскільки їх можна пов'язати з конкретним користувачем та ідентифікувати його особу за інформацією провайдера. В основі лежить підхід вразливості цих даних, коли будь-який фрагмент інформації у поєднані з іншими даними може привести до втрати анонімності особи. Навіть припущення непрямої ідентифікації особи є достатнім для того, щоб ці дані захищати. Тобто такі складові, як URL-адреса та IP-адреса та інші технічні дані, мають вважатися персональними даними мережевого профілю особи та надійно захищатися від збору, аналізу та розповсюдження.

У межах відносин у мережевому просторі верифікація є етапом підтвердження зв'язку між профілем користувача та його власником. Ідентифікація фізичної особи базується на поєднанні її персональних даних, конфіденційної та публічної інформації, а також технічних ідентифікаторів (табл. 1).

У таблиці 1 наведена фактична архітектура роботи електронних систем трекінгу, рекламних платформ та розвідувальних сервісів, які завдяки сукупному накопиченню, накладенню та перетину непов'язаних між собою і окремо нешкідливих категорій даних створюють профіль, що є не менш точним, ніж паспортні дані користувача комунікаційного пристрою.

Логіка поєднання категорій (див. табл. 1) дозволяє виявити стабільні цифрові профілі користувачів комунікаційних пристроїв, навіть за відсутності прямих ідентифікаторів. Умовно можна об'єднати категорії за рівнями:

Рівень 1 – технічний опис комунікаційного пристрою (категорії 3 та 4) включає: **Мережеві ідентифікатори** (IP, MAC) + **Відбитки пристроїв** (IMEI, User-Agent, конфігурація апаратної частини). Ці дані формують унікальний «технічний паспорт» комунікаційного пристрою. Навіть якщо користувач видалив файли cookie, веббраузер повідомляє: версію операційної системи (ОС), роздільну здатність екрана, перелік шрифтів, часовий пояс, параметри графічного процесора (рис. 1).

Передача даних про графічний процесор відбувається під час взаємодії комунікаційного пристрою з будь-яким інтернет-ресурсом (див.

Таблиця 1

Багаторівневий комплекс даних для ідентифікації фізичної особи у мережевому середовищі

№	Категорія даних	Елементи даних	Рівень ідентифікації	Типові джерела	Рівень ризику для конфіденційності
1	Прямі ідентифікатори	ПІБ, дата народження, паспортні дані, адреса, телефон, електронна пошта	Дуже високий	Державні реєстри, форми реєстрації	критичний
2	Ідентифікатори облікових записів	User ID, логін, OAuth токени, Cookie ID, Advertising ID	високий	Вебсервіси, мобільні застосунки	високий
3	Мережеві ідентифікатори	IP-адреса, MAC-адреса, DNS-запити, геолокація	середній–високий	Провайдери, мережеві журнали, трафік	високий
4	Відбитки пристроїв	IMEI, Android ID, IDFA, User-Agent, конфігурація обладнання	високий	Мобільні ОС, веббраузери	критичний
5	Поведінкові дані	Патерни вводу, активність, часові характеристики	середній	Логи застосунків, аналітичні системи	середній – високий
6	Дані контенту	Тексти, зображення, відео, метадані (EXIF)	середній	Соціальні мережі, хмарні сервіси	високий
7	Соціальна взаємодія	Контакти, зв'язки, взаємодія	середній – високий	Соціальні мережі, месенджери	високий
8	Біометричні ідентифікатори	Відбитки пальців, обличчя, голос, райдужна оболонка ока	Дуже високий	Біометричні системи	критичний
9	Обчислені дані	Інтереси, поведінка, психографіка	середній	Аналітичні платформи	середній – високий

Рис. 1. Основні канали збору даних про графічний процесор комунікаційного пристрою

рис. 1). Для здійснення цієї процедури використовуються такі канали:

• WebGL – за допомогою запитів getParameter (RENDERER) та getParameter(VENDOR) отримує точну інформацію про марку, модель та версією драйвера. Цей процес відбувається автоматично без будь-яких дозволів чи заборон з боку користувача;

• Canvas – веббраузер малює невидиме зображення з текстом та градієнтами, а потім зчитує пікселі. Кожен графічний процесор виконує рендеринг субпікселів та згладжування пікселів по-власному, що дозволяє сформувати унікальний хеш комунікаційного пристрою на основі комбінації «графічний процесор + драйвер + ОС»;

• WebGPU надає дані про GPUAdapter у структурі запитуваного об'єкта adapterInfo з полями vendor, architecture, device та description;

• непрямі канали дають змогу визначити час виконання тестових обчислювальних шейдерів, що дозволяє опосередковано обчислити кількість обчислювальних ядер GPU. Також виявляється тип дисплея (Retina, HiDPI), підтримка HDR та клас комунікаційного пристрою.

Рівень 2 – поведінковий рівень (категорії 5 + 7): **Поведінкові дані** (шаблони введення, час активності) + **Соціальна взаємодія** (з ким спілкується, як часто) створюють «поведінковий зліпок». Користувач комунікаційного пристрою натискає клавіші з однаковим ритмом, гортає сторінки зі звичною швидкістю, листується з одним і тим самим колом контактів – навіть під новим акаунтом.

Рівень 3 – інтерференційний шар (категорії 6 + 9): **Дані контенту** (тексти, фото с EXIF) + **Обчислені дані** (інтереси, поведінка, психографіка). Ці дані дають змогу визначити те, що явно не вказано. EXIF-дані фотографії надають координати та час зйомки; стиль написання – демографічні дані; регулярність публікацій – робочий графік тощо (Zadereyko et al., 2017).

Отже, технічні дані, які збираються з комунікаційного пристрою користувача, автоматично набувають статус його унікальних ідентифікаторів (див табл. 1). Вони автоматично генеруються комунікаційним пристроєм та збираються електронними сервісами в процесі взаємодії його ОС та застосунків (Zadereyko et al., 2020). Саме ці дані формують унікальний цифровий

профіль (відбиток) комунікаційного пристрою користувача у мережевому просторі.

Організація захисту комунікаційних пристроїв від витоків персональних даних. Сукупність наведених вище аргументів дозволяє сформулювати обґрунтування потреби захисту від витоків персональних даних із комунікаційних пристроїв користувачів.

В основу організації такого захисту слід покласти принцип мінімізації даних, закріплений у європейському Загальному регламенті про захист даних (GDPR). Стосовно комунікаційних пристроїв він передбачає, що пристрій або застосунок запитує винятково ті дозволи (мережеві з'єднання), які функціонально необхідні для його роботи, а користувач, у свою чергу, критично оцінює обґрунтованість кожного запиту та ухвалює остаточне рішення щодо його дозволу або блокування.

Для вирішення цього завдання на практиці найбільш функціональним засобом є мережевий екран як елемент багаторівневої системи безпеки. Його принципова перевага полягає в тому, що він здійснює контроль на рівні мережевої взаємодії комунікаційного пристрою – незалежно від того, яким саме модулем ОС або застосунком ініційовано передачу даних і який її заявлений характер. Тим самим мережевий екран виступає компенсуючим контролем, що нейтралізує загрози, які не були передбачені на рівні управління дозволами застосунків.

Найпоширенішою архітектурною реалізацією мережевого екрана є використання локального VPN-інтерфейсу. Цей підхід використовує VPN API ОС для перехоплення та перевірки мережевого трафіку безпосередньо на комунікаційному пристрої (рис. 2).

З технічної точки зору комунікаційний пристрій встановлює VPN-тунель на інтерфейс, що дозволяє мережевому екрану виступати у ролі локального проксі-сервера. Головною перевагою цієї архітектури є те, що весь мережевий трафік залишається на комунікаційному пристрої і не передається стороннім суб'єктам мережевого середовища.

Реалізація цього підходу втілена у застосунках NetGuard (NetGuard – no-root firewall, 2026) для ОС Android і у Lockdown Privacy (Lockdown Privacy: AdBlock VPN, 2026) для ОС iOS.

Організація ефективного захисту на рівні розглянутих застосунків передбачає не лише початкову конфігурацію правил фільтрації мережевих з'єднань, а й систематичний моніторинг мережевої активності комунікаційного

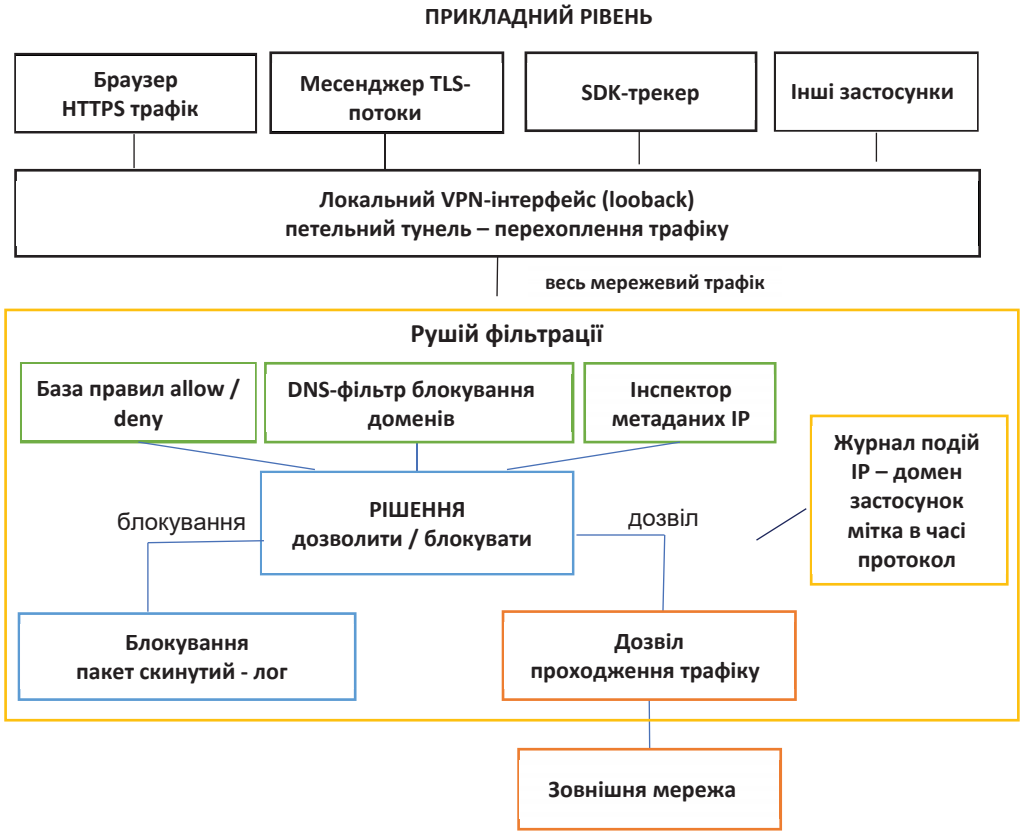

Рис. 2. Принцип функціонування мережевого екрана на локальному VPN-інтерфейсі комунікаційного пристрою

пристрою. Вихідні з'єднання, що реєструються мережевим екраном, є цінним джерелом інформації для виявлення аномальної мережевої активності:

- надзвичайно високої частоти з'єднань;
- передача даних у нетиповий час;
- запити до невідомих доменів/IP-адрес;
- запити застосунків на з'єднання з доменами/IP-адресами, які не мають до них явного відношення.

Постійний моніторинг цих з'єднань дозволяє своєчасно виявляти ймовірні витоки даних та перевіряти працездатність комунікаційного пристрою після їх блокування (табл. 2).

Таблиця 2

Результати моніторингу мережевих з'єднань комунікаційних пристроїв

Категорія збору даних	Домен/IP-адреса	Категорія	Власник	Які дані збираються	Працездатність у разі блокування мережевого з'єднання (+/-)
1	2	3	4	5	6
Web серфінг	google-analytics.com	Аналітика	Google	Відвідування інтернет-ресурсів, поведінка користувача, джерела трафіку, події	+
	analytics.google.com			GA4: сесії, конверсії, user-ID	+
	stats.g.doubleclick.net			Міжсайтове відстеження, рекламні конверсії	+
	googletagmanager.com			Контейнер тегів – завантажує інші трекери	+
	ssl.google-analytics.com			HTTPS- кінцева точка Universal Analytics	+
	googleads.g.doubleclick.net	Реклама		Google Ads: ремаркетинг, конверсії	+
	adservice.google.com	Реклама		Міжсайтовий ідентифіка-тор для персоналізованої реклами	+
	googleadservices.com	Реклама		Фіксація рекламних уподобань користувача	+
	static.doubleclick.net	Реклама	Google	Показ цільової реклами на основі уподобань користувача	+
	browser-intake-datadoghq.eu	Аналітика	Datadog	Збір даних про показники продуктивності пристрою	+
ОС iOS	firebaselogging-pa.googleapis.com	Аналітика	Google	Надсилає телеметрію та діагностичні дані на сервери Google	+
	crashlytics.com	Аналітика		Відстеження збоїв у роботі застосунків	+
	app-analytics-services.com	Аналітика		Збір аналітичних даних із вебсайтів та застосунків	+
	ca.iadsdk.apple.com	Реклама	Apple	Відстежує дії користувача для проведення рекламних кампаній	+
	firebaseappcheck.googleapis.com	Аналітика		Перевірка пристрою	-
	appsflyersdk.com	Аналітика	AppsFlyer	Відстеження поведінки користувачів у застосунках	+

Продовження таблиці 2

1	2	3	4	5	6
ОС Android	1e.100.net	Аналітика	Google	Відстеження поведінки користувачів у застосунках	+
	android.googleapis.com	Системна		Регістрація пристрою, push-повідомлення GCM/FCM	+
	googleapis.com	Системна		API Google: геолокація, аутентифікація, карти	+
	googleadservices.com	Реклама		Google Ads SDK: персоналізована реклама	+
	adservice.google.com	Реклама		Міжсайтовий ID, таргетингової реклами	+

На основі результатів проведеного моніторингу мережевих з'єднань комунікаційних пристроїв під управлінням ОС Android та iOS у режимі класичного вебсерфінгу можна стверджувати, що їх можна розділити на два класи:

• **аналітика** (моніторинг стану комунікаційного пристрою та поведінкових факторів користувача) – google-analytics.com, analytics.google.com, ssl.google-analytics.com, googletagmanager.com, firebaselogging-pa. googleapis.com, crashlytics.com, app-analytics-services.com, browser-intake-datadoghq.eu;

• **реклама** (монетизація на основі результатів моніторингу): stats.g.doubleclick.net, googleads.g.doubleclick.net, adservice.google.com, googleadservices.com, static.doubleclick.net.

Загалом результати аналізу мережевих з'єднань (див. табл. 2) переконливо демонструють типові процеси взаємодії на рівні інформаційно-комунікаційних систем, де:

1) у мережеве середовище з комунікаційного пристрою користувача постійно передаються дані:

– про безпосередні дії користувача;
– про дії в мережевому середовищі;
– про відвідані інтернет-ресурси;
– про рекламні вподобання;
– про технічний стан пристрою;

2) блокування практично всіх з'єднань не порушує функціональну працездатність комунікаційного пристрою.

Отже, організація захисту від витоку персональних даних з комунікаційного пристрою за допомогою мережевого екрана є комплексним технічним завданням, рішення якого потребує послідовного застосування таких етапів:

• вибір архітектурної моделі – локального VPN-екрана;

• усталені конфігурації правил фільтрації мережевих з'єднань сервісів (див. табл. 2);

• засновані на принципі заборони та гранулярним управлінням доступом застосунків, забезпечує найбільш повний контроль над мережевою активністю;

• систематичний моніторинг та регулярна актуалізація правил фільтрації мережевих з'єднань.

Разом з цим варто визнавати принципове обмеження розглянутого підходу: мережевий екран контролює мережеву взаємодію, але не усуває причини надлишкового збору даних, закладеного в архітектурі ОС та їх застосунків, а також у бізнес-моделях аналітично-рекламних сервісів. У цьому сенсі застосування мережевого екрана є необхідним, проте недостатнім елементом комплексної стратегії захисту від витоків персональних даних користувачів, яка неминуче має бути закріпленою у правових, організаційних та освітніх компонентах держави.

Висновки та перспективи подальших досліджень. У рамках дослідження стану захисту персональних даних у мережевому середовищі систематизовано дані, які складають основу ідентифікації особи. За результатами аналізу захищеності цих даних виділено основні чотири групи, а саме: персональні дані, конфіденційна інформація, публічна інформація та технічні ідентифікатори. Виокремлення технічних ідентифікаторів в окрему категорію пов'язано з тим, що ці дані у поєднанні з персоналізованою інформацією надають можливість прямо або опосередковано ідентифікувати особу у мережевому середовищі.

Отже, систематизацію ідентифікаторів мережевого профілю особи у мережевому середовищі здійснено залежно від категорії даних, які можуть бути використані у процесі верифікації (див. табл. 1):

• **прямі ідентифікатори**, що дають змогу однозначно ідентифікувати користувача:

– ідентифікаційні дані фізичної особи (зокрема, прізвище, ім'я та по батькові, дата народження, серія та номер паспорта або ID-картка, відомості про місце проживання або місце перебування, електронна адреса, номер мобільного телефону);

– біометричні дані, які підтверджують те, що цифровим профілем володіє саме та людина, яка його подає (FaceID, відбитки пальців, голос, райдужна оболонка ока);

– облікові дані фізичних осіб у базах даних публічних електронних реєстрів та облікові дані, які використовуються при перевірці та захисті доступу до профілю (автентифікація): логін, пароль, криптографічні ключі;

• **ідентифікатори комунікаційних пристроїв**, які в поєднанні з іншими даними надають можливість ідентифікувати особу:

– відбитки комунікаційних пристроїв формуються його технічними параметрами;

– мережеві ідентифікатори формуються IP-адресою (геолокацією), MAC-адресою, DNS-запитами, які фіксуються провайдером;

– обчислені дані використовують для аналізу уподобань та поведінки, що вказує на потенційну загрозу втрати конфіденційності;

• **поведінкові ідентифікатори користувачів** через унікальні патерни дозволяють опосередковано ідентифікувати особу:

– соціальна взаємодія – це дані про цифрові профілі користувачів, на підставі яких здійснюється моніторинг загроз, нетипових дій, підозрілої активності;

– дані контенту формують «цифровий портрет» особи або її дії, які можуть бути використані проти неї;

– поведінкові дані надають можливість прогнозувати активність користувача для її подальшого використання.

В умовах сучасної цифровізації суспільства, надзвичайного та воєнного стану захист персональних даних стає важливим елементом забезпечення інформаційної безпеки України і вимагає дотримання підвищеного рівня захищеності, конфіденційності, зберігання й особливих умов передачі на території держави та за її межами. Постійний процес обміну даними між суб'єктами зумовлює виникнення загроз порушення конфіденційності.

Результати дослідження свідчать про те, що ефективний захист персональних даних особи можливо здійснити тільки за поєднання правових, організаційних і технічних заходів. Важливу роль відіграє розвиток технологій та впровадження підходів щодо мінімізації витоку даних із комунікаційних пристроїв користувачів. При цьому важливою умовою ефективності такого підходу є підвищення цифрової грамотності користувачів – здатності усвідомлено оцінювати ризики й ухвалювати оптимальні рішення для захисту в мережевому середовищі.

Подальший аналіз цієї проблематики спрямований на вивчення технологій несанкціонованого збору персональних даних із комунікаційних пристроїв користувачів. Це дозволить сформувати системний підхід, заснований на інтеграції принципів мінімізації витоків даних, проєктування з урахуванням необхідного рівня конфіденційності, децентралізованої обробки інформації та реального контролю з боку користувачів в єдину архітектуру захисту персональних даних.

ЛІТЕРАТУРА:

1. Про інформацію: закон України від 02.10.1992 р. № 2657-XII. *Верховна Рада України*: офіц. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення 07.04.2026)

2. Про захист персональних даних : закон України від 01.06.2010 р. № 2297-VI. *Верховна Рада України*: офіц. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення 07.04.2026)

3. Про доступ до публічної інформації : закон України від 13.01.2011 р. № 2939-VI. *Верховна Рада України*: офіц. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення 07.04.2026)

4. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г. Устименка) від 30 жовт. 1997 р. № 5-зп. *Верховна Рада України*: офіц. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/v005p710-97#Text (дата звернення 07.04.2026)

5. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України № 2-рп/2012 від 20.01.2012 року. *Верховна Рада України*: офіц. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Tex (дата звернення 07.04.2026)

6. General Data Protection Regulation (EU GDPR). The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). *EUR-lex*. URL: https://gdpr-text.com/ (дата звернення 09.04.2026)

7. Zadereyko O., Trofymenko O., Prokop Yu., Loginova N., Dyka A., Kukharenko S. Research of potential data leaks in information and communication systems. *RADIOELECTRONIC AND COMPUTER SYSTEMS.* 2022. № 4(104). P. 64-84. DOI: https://doi.org/10.32620/reks.2022.4.05.

8. Задерейко О.В., Трофименко О.Г., Єленич С.І., Логінова Н.І., Гура В.І. Системний аналіз захищеності державних електронних реєстрів та баз персональних даних. *Кібербезпека: освіта, наука, техніка*. 2025. № 4(28). С. 57–70. DOI: https://doi.org/10.28925/2663-4023.2025.28.735

9. Про електронну ідентифікацію та електронні довірчі послуги : закон України від 05 жовтня 2017 р. № 2155 VIII. *Верховна Рада України* : офіц. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення 03.04.2026)

10. Про затвердження Положення про інтегровану систему електронної ідентифікації : постанова Кабінету Міністрів України від 03 листоп. 2023 р. № 1150. *Верховна Рада України* : офіц. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/1150-2023-%D0%BF#Text (дата звернення 03.04.2026)

11. Spevakov A.G., Spevakova S.V., Primenko D.V. Method of data depersonalization in protected automated information systems. *Radio Electronics, Computer Science, Control.* 2020. № 1. P. 162–168. DOI: https://doi.org/10.15588/1607-3274-2020-1-16

12. Bogdanov A., Shchegoleva N., Khvatov V., Dik G., Kiyamov J., Dik A. K-anonymity versus PSI3 for depersonalization and security assessment of large data structures. *International Conference on Computational Science and Its Applications*. 2023, June. P. 317–333. DOI: https://doi.org/10.1007/978-3-031-37120-2_21

13. Dalal A., Kaushik K., Polagani S. S., Upadhyay L., Soni M. Privacy-preserving techniques in data anonymization and masking: Trends and challenges. *Smart Technologies and Intelligent Computing*. 2026. P. 336–345. DOI: https://doi.org/10.1201/9781003666929-48

14. Nayak S. K., Ojha A. C. Data leakage detection and prevention: Review and research directions. *Machine learning and information processing: proceedings of ICMLIP 2019*. 2020. P. 203–212. URL: https://link.springer.com/chapter/10.1007/978-981-15-1884-3_19 (дата звернення 02.04.2026)

15. Saqib N. A., Abbasi E. G., Rubaian G. A. B., Aloneizi M. A., Alotaibi R. M., Alasmari L. N. Detection of Personally Identifiable Information Leakage on the Web Using Artificial Intelligence Techniques: A Comprehensive Review. In *2025 3rd International Conference on Business Analytics for Technology and Security (ICBATS).* 2025, May. P. 1–8. IEEE. DOI: https://doi.org/10.1109/ICBATS66542.2025.11258366

16. Quach S., Thaichon P., Martin K. D., Weaven S., & Palmatier R. W. Digital technologies: tensions in privacy and data. Journal of the academy of marketing science. 2022. № 50(6). P.1299–1323. DOI: https://doi.org/10.1007/s11747-022-00845-y

17. Zadereyko A., Loginova N., Troyanskiy A., Trofymenko O. The implementation of depersonalization algorithm of digital images. *2nd International Conference on Advanced Information and Communication Technologies-2017* (AICT-2017), Lviv, Ukraine, July 4–7. 2017. P. 56–61. DOI: https://doi.org/10.1109/AIACT.2017.8020065

18. NetGuard - no-root firewall. URL: https://netguard.me/

19. Lockdown Privacy: AdBlock VPN. URL: https://apps.apple.com/us/app/lockdown-privacy-adblock-vpn/id1469783711

REFERENCES

1. Pro informatsiiu: zakon Ukrainy vid 02 zhovt. 1992 r. № 2657-XII. *Verkhovna Rada Ukrainy*: ofits. vebsait. https://zakon.rada.gov.ua/laws/show/2657-12#Text

2. Pro zakhyst personalnykh danykh : zakon Ukrainy vid 01 cherv. 2010. № 2297-VI. *Verkhovna Rada Ukrainy*: ofits. vebsait. https://zakon.rada.gov.ua/laws/show/2297-17

3. Pro dostup do publichnoi informatsii : zakon Ukrainy vid 13 sich. 2011. № 2939-VI. Verkhovna Rada Ukrainy: ofits. vebsait. https://zakon.rada.gov.ua/laws/show/2939-17

4. Rishennia Konstytutsiinoho Sudu Ukrainy u spravi shchodo ofitsiinoho tlumachennia statei 3, 23, 31, 47, 48 Zakonu Ukrainy «Pro informatsiiu» ta statti 12 Zakonu Ukrainy «Pro prokuraturu» (sprava K.H. Ustymenka) vid 30 zhovt. 1997 r. № 5-zp. *Verkhovna Rada Ukrainy*: ofits. vebsait. https://zakon.rada.gov.ua/laws/show/v005p710-97#Text

5. Rishennia Konstytutsiinoho Sudu Ukrainy u spravi za konstytutsiinym podanniam Zhashkivskoi raionnoi rady Cherkaskoi oblasti shchodo ofitsiinoho tlumachennia polozhen chastyn pershoi, druhoi statti 32, chastyn druhoi, tretoi statti 34 Konstytutsii Ukrainy № 2-rp/2012 vid 20.01.2012 roku. *Verkhovna Rada Ukrainy :* ofits. vebsait. https://zakon.rada.gov.ua/laws/show/v002p710-12

6. General Data Protection Regulation (EU GDPR). The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, 2 ((EU) 2016/679). *EUR-lex*. https://gdpr-text.com/

7. Zadereyko, O., Trofymenko, O., Prokop, Yu., Loginova, N., Dyka, A., & Kukharenko, S. (2022). Research of potential data leaks in information and communication systems. *Radioelectronic and computer systems,* 4(104), 64–84. https://doi.org/10.32620/reks.2022.4.05.

8. Zadereyko, O., Trofymenko, O., Yelenych, S., Loginova, N., & Hura, V. (2025). Systematic analysis of the security of state electronic registers and personal databases. *Cybersecurity: Education, Science, Technique*, 4(28), 57–70. https://doi.org/10.28925/2663-4023.2025.28.735

9. Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy : zakon Ukrainy vid 05 zhovtnia 2017 r. № 2155 VIII. *Verkhovna Rada Ukrainy* : ofits. vebsait. https://zakon.rada.gov.ua/laws/show/2155-19#Text

10. Pro zatverdzhennia Polozhennia pro intehrovanu systemu elektronnoi identyfikatsii : postanova Kabinetu Ministriv Ukrainy vid 03 lystop. 2023 r. № 1150. *Verkhovna Rada Ukrainy* : ofits. vebsait. https://zakon.rada.gov.ua/laws/show/1150-2023-%D0%BF#Text

11. Spevakov, A.G., Spevakova, S.V., & Primenko, D.V. (2020). Method of data depersonalization in protected automated information systems. *Radio Electronics, Computer Science, Control*, 1, 162–168. https://doi.org/10.15588/1607-3274-2020-1-16

12. Bogdanov, A., Shchegoleva, N., Khvatov, V., Dik, G., Kiyamov, J., & Dik, A. (2023, June). K-anonymity versus PSI3 for depersonalization and security assessment of large data structures. *In International Conference on Computational Science and Its Applications*, 317–333. https://doi.org/10.1007/978-3-031-37120-2_21

13. Dalal, A., Kaushik, K., Polagani, S. S., Upadhyay, L., & Soni, M. (2026). Privacy-preserving techniques in data anonymization and masking: Trends and challenges. *Smart Technologies and Intelligent Computing*, 336–345. https://doi.org/10.1201/9781003666929-48

14. Nayak, S. K., & Ojha, A. C. (2020). Data leakage detection and prevention: Review and research directions. *Machine learning and information processing: proceedings of ICMLIP 2019*, 203–212. https://link.springer.com/chapter/10.1007/978-981-15-1884-3_19

15. Saqib, N. A., Abbasi, E. G., Rubaian, G. A. B., Aloneizi, M. A., Alotaibi, R. M., & Alasmari, L. N. (2025, May). Detection of Personally Identifiable Information Leakage on the Web Using Artificial Intelligence Techniques: A Comprehensive Review. *3rd IEEE International Conference on Business Analytics for Technology and Security (ICBATS'2025)*, 1–8. https://doi.org/10.1109/ICBATS66542.2025.11258366

16. Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the academy of marketing science*, 50(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

17. Zadereyko, A., Loginova, N., Troyanskiy, A., Trofimenko, E. (2017). The implementation of depersonalization algorithm of digital images. *2nd International Conference on Advanced Information and Communication Technologies-2017* (AICT), Lviv, Ukraine, July 4–7, 56–61. https://doi.org/10.1109/AIACT.2017.8020065

18. NetGuard - no-root firewall. https://netguard.me/

19. Lockdown Privacy: AdBlock VPN. https://apps.apple.com/us/app/lockdown-privacy-adblock-vpn/id1469783711

Дата першого надходження статті до видання: 17.04.2026
Дата прийняття статті до друку після рецензування: 11.05.2026
Дата публікації (оприлюднення) статті: 29.05.2026