Сучасні способи незаконного заволодіння персональними даними: правові виклики та ризики у цифрову епоху*

Думчиков М. О.[1]

Опубліковано	Секція	УДК
20.02.2025	Право	343.9

DOI: https://doi.org/10.5281/zenodo.14898865

Анотація. У статті досліджуються сучасні методи незаконного заволодіння персональними даними, що становлять одну з найсерйозніших загроз інформаційній безпеці у цифрову епоху. Автором проаналізовано ключові способи, які використовуються кіберзлочинцями, зокрема фішинг, смішинг, атаки через Wi-Fi-мережі, використання шкідливого програмного забезпечення та мобільних застосунків. Зазначено, що персональні дані стають стратегічно важливим ресурсом, який активно використовується не лише для фінансового шахрайства, а й для маніпулювання громадською думкою, підриву довіри до державних інституцій та здійснення гібридних атак.

З огляду на глобальні тенденції розвитку кіберзлочинності, автор звертає увагу на те, що традиційні методи правового регулювання не завжди встигають за швидкими технологічними змінами. У статті окреслено основні виклики для правової системи, пов'язані з розширенням масштабів використання кіберзлочинних інструментів, а також наведено приклади актуальних загроз в Україні. Особливу увагу приділено тому, як російська агресія посилила ризики використання персональних даних для дезінформаційних кампаній та шпигунства.

Автор наголошує, що одним із найбільш ефективних методів протидії є підвищення рівня цифрової грамотності серед населення, оскільки саме людський фактор залишається ключовою вразливістю, яку експлуатують зловмисники. У статті також запропоновано комплексні заходи з кібербезпеки, які включають посилення державного контролю за обробкою та зберіганням персональних даних, розробку ефективних механізмів моніторингу кіберзлочинів та впровадження жорсткіших вимог до розробників цифрових сервісів.

Ключові слова: кібербезпека, персональні дані, фішинг, смішинг, шкідливе програмне забезпечення, соціальна інженерія, цифрова грамотність, правове регулювання кіберзлочинності.

* *Робота виконана в рамках проєкту «Інтеграційна парадигма цифрової трансформації в системі протидії фінансовій злочинності: синергетичний підхід до превенції та боротьби» (номер державної реєстрації 0125U000602)*

[1] Д.ю.н., доцент, доцент кафедри кримінально правових дисциплін та судочинства Навчально-наукового інституту права СумДУ , https://orcid.org/0000-0002-4244-2419

Modern Methods of Illegal Acquisition of Personal Data: Legal Challenges and Risks in the Digital Age

Abstract. The article examines modern methods of unlawful acquisition of personal data, which represent one of the most serious threats to information security in the digital age. The author analyzes the key techniques used by cybercriminals, including phishing, smishing, Wi-Fi network attacks, the use of malicious software, and mobile applications. It is noted that personal data has become a strategically important resource, actively exploited not only for financial fraud but also for manipulating public opinion, undermining trust in state institutions, and conducting hybrid attacks.

Considering global trends in cybercrime development, the author highlights that traditional legal regulation methods often fail to keep pace with rapid technological changes. The article outlines the main challenges facing the legal system due to the expanding use of cybercriminal tools and provides examples of current threats in Ukraine. Particular attention is given to how Russian aggression has exacerbated the risks of using personal data for disinformation campaigns and espionage.

The author emphasizes that one of the most effective countermeasures is enhancing digital literacy among the population, as the human factor remains a key vulnerability exploited by malicious actors. The article also proposes comprehensive cybersecurity measures, including strengthening state control over the processing and storage of personal data, developing effective mechanisms for monitoring cybercrimes, and introducing stricter requirements for digital service developers.

Keywords: cybersecurity, personal data, phishing, smishing, malicious software, social engineering, digital literacy, legal regulation of cybercrime.

Вступ

Постановка проблеми. Динамічний розвиток інформаційно-телекомунікаційних технологій сприяє трансформації всіх сфер суспільного життя, забезпечуючи нові можливості для економічного, соціального та культурного прогресу. Варто наголосити, шо цифровізація стала невід'ємною складовою сучасної реальності, змінюючи форми взаємодії між людьми, бізнесом і державними інституціями. Водночас, поряд із перевагами цифрової епохи, стрімко зростає кількість загроз, пов'язаних із безпекою інформації та правовим захистом персональних даних.

Сьогодні, з впевненістю можна казати, що персональні дані стали стратегічно важливим активом, що привертає увагу зловмисників, які використовують різноманітні способи незаконного їх заволодіння. Водночас, використання сучасних кіберзлочинних технологій, зокрема фішингу, соціальної інженерії, шкідливого програмного забезпечення та зламів баз даних, створює серйозні виклики для правової системи. Особливо загрозливими на наше переконання є масштабні витоки інформації, що спричиняють фінансові збитки, порушення конфіденційності та використання викрадених даних у шахрайських схемах.

Актуальність проблеми посилюється тим, що традиційні правові механізми часто не встигають за технологічними змінами, а заходи державного регулювання та міжнародного співробітництва потребують постійного удосконалення. В умовах цифрової епохи, коли значна частина життєдіяльності людини відбувається в онлайн-середовищі, захист персональних даних перетворюється на першочерговий пріоритет як для окремих громадян, так і для держави в цілому.

Стан дослідження. Проблематика дослідження способів і методів незаконного заволодіння персональними даними як одного з різновидів кіберзлочинності є предметом наукового інтересу багатьох вітчизняних і зарубіжних науковців, зокрема, Мельник К.С, Саєнко М.І., Гринько Л.П., Akanbi Caleb, Dumitrasc V., Serral-Gracià R.

Водночас, з огляду на динаміку розвитку цифрового середовища та постійне вдосконалення тактик кіберзлочинців, ця проблема залишається актуальною та потребує подальшого глибокого наукового аналізу.

Метою дослідження є аналіз сучасних способів незаконного заволодіння персональними даними, виявлення основних правових викликів і ризиків у цифрову епоху та розробка рекомендацій щодо підвищення ефективності їх правового захисту.

Результати

Висновок**.** Розвиток цифрових технологій кардинально змінив способи обробки, зберігання та передачі персональних даних. Сучасні інформаційні системи дозволяють миттєво обмінюватися великими обсягами даних, що значно підвищує ефективність як комерційної, так і державної діяльності. Водночас, широке впровадження цифрових рішень створює нові ризики, зокрема щодо безпеки персональної інформації.

Неконтрольоване поширення даних, зростаюча залежність від цифрових платформ і недостатня правова регламентація сприяють активному використанню персональних відомостей у незаконних схемах.

Варто зауважити, що кіберзлочинці дедалі частіше використовують передові техніки для несанкціонованого доступу до персональних даних, розширюючи масштаби кіберзагроз. Все це посилюється використанням генеративних систем штучного інтелекту, автоматизованих бот-мереж, а також вразливостей у програмному забезпеченні, як результат значне ускладнення ідентифікації злочинців і притягнення їх до відповідальності.

На наше переконання, ситуація в Україні має унікальні особливості, що зумовлюють специфічні виклики у сфері захисту персональних даних. Зокрема, в умовах повномасштабного вторгнення російської федерації питання кібербезпеки набуло критично важливого значення. Кібератаки, спрямовані на державні органи, підприємства та громадянське суспільство, вже давно перестали бути лише проявом кіберзлочинності. Ми переконані, що сьогодні вони є невід'ємною частиною гібридної війни, яка має на меті дестабілізацію українського суспільства, підрив довіри до державних інституцій та ослаблення інформаційного простору.

Водночас зловмисники дедалі активніше використовують викрадені персональні дані громадян для досягнення стратегічних цілей. На нашу думку, це створює передумови для широкомасштабних інформаційних маніпуляцій, поширення дезінформації та підриву соціальної згуртованості. Окрім того, існує безпосередня загроза для критичної інфраструктури держави, що може мати як політичні, так і економічні наслідки. В ході нашого дослідження ми вважаємо за необхідне не лише проаналізувати основні способи незаконного заволодіння персональними даними, а й запропонувати правові механізми, спрямовані на зміцнення кіберстійкості України та ефективний захист інформаційного простору.

Як свідчить статистика кіберзлочинності, проблема незаконного заволодіння персональними даними набуває загрозливих масштабів. За даними Федерального бюро розслідувань США, у 2022 році було зафіксовано 800 944 скарги на кіберзлочини, що торкнулися щонайменше 422 мільйонів осіб. Водночас, прогнозується, що у 2023 році кількість зламаних облікових записів сягне приблизно 33 мільярдів, а сукупні збитки від подібних порушень можуть перевищити 8 трильйонів доларів [1].

На нашу думку, така тенденція свідчить про системне посилення загроз у сфері інформаційної безпеки, зокрема незаконного отримання персональних даних. За прогнозами, до 2025 року збитки від кіберзлочинів можуть сягнути 10,5 трильйона доларів, що робить їх однією з найбільш значущих глобальних загроз [2].

Варто зазначити, що 80% усіх зареєстрованих кіберзлочинів, як правило, пов'язані з фішинговими атаками. Водночас, фішинг залишається другою за поширеністю

причиною витоків даних і найдорожчим видом порушень, середня вартість яких оцінюється у 4,91 мільйона доларів. Аналізуючи наведені дані, можна зробити висновок, що сучасні способи незаконного заволодіння персональними даними є не лише інструментом фінансового шахрайства, а й потужним механізмом кіберзагроз, які можуть мати як економічні, так і безпекові наслідки [3].

На наше переконання, основними жертвами подібних злочинів залишаються користувачі соціальних мереж, онлайн-банкінгу та цифрових платформ. Це зумовлено як низьким рівнем обізнаності про кіберризики, так і недостатнім рівнем безпеки з боку самих онлайн-сервісів. Водночас, в Україні ця проблема набула особливої гостроти у зв'язку з повномасштабною війною, що значно посилило вразливість громадян і державних інституцій перед кібератаками. Як свідчать аналітичні дані, у 2022–2023 роках було зафіксовано суттєве зростання кількості інцидентів, пов'язаних із викраденням персональних даних, що стали частиною гібридної агресії. У ході таких атак зловмисники прагнули отримати доступ до конфіденційної інформації громадян, військовослужбовців, державних службовців та працівників критичної інфраструктури, що створило додаткові загрози національній безпеці [4].

Як свідчить аналіз тенденцій у сфері кібербезпеки, зростання кількості кібератак, спрямованих на незаконне заволодіння персональними даними, є закономірним наслідком удосконалення зловмисниками своїх методів і технологій. На наше переконання, ця загроза набуває особливої актуальності в умовах цифровізації всіх сфер суспільного життя, коли обсяг оброблюваної та збереженої персональної інформації стрімко зростає.

Використання зловмисниками широкого спектра інструментів, що поєднують технічні засоби та методи соціальної інженерії, значно ускладнює виявлення та нейтралізацію таких атак. Ми переконані, що постійна еволюція кіберзагроз, адаптація «хакерів» до нових технологій, експлуатація вразливостей у програмному забезпеченні та активне використання штучного інтелекту створюють нові виклики для інформаційної безпеки.

Водночас ефективність заходів протидії значною мірою залежить від рівня обізнаності користувачів, державної політики у сфері кібербезпеки та якості міжнародної координації у боротьбі з кіберзлочинністю. Беручи до уваги зазначене, розглянемо найбільш поширені та небезпечні способи незаконного заволодіння персональними даними.

Фішинг є одним із найбільш поширених і небезпечних способів незаконного заволодіння персональними даними, який ґрунтується на введенні користувача в оману шляхом створення підроблених вебсайтів або розсилки електронних листів і повідомлень, які імітують надійні джерела, зокрема фінансові установи, популярні сервіси або державні органи. Основною метою фішингу є виманювання конфіденційної інформації, такої як логіни, паролі, дані банківських карток, реквізити для доступу до облікових записів або особисті документи [5].

Ми переконані, що особлива небезпека фішингу полягає в масовому характері цієї техніки та здатності вводити в оману навіть досвідчених користувачів. Зловмисники активно застосовують різні психологічні прийоми, зокрема створення почуття терміновості або загрози втрати доступу до облікових записів. Найпоширенішими прикладами таких маніпуляцій є повідомлення з текстом на кшталт: «Ваш обліковий запис буде заблоковано. Підтвердіть дані» або «Ваша банківська картка скомпрометована. Терміново змініть пароль». Водночас вони можуть використовувати індивідуальний підхід, зокрема персоналізовані повідомлення, які створюють ілюзію довіри до джерела інформації.

На наше переконання, актуальність проблеми фішингу в Україні значно зросла у контексті повномасштабного вторгнення російської федерації. З 2022 року значна

частина кібератак, спрямованих на громадян і державні органи, включала фішингові кампанії з метою отримання даних військовослужбовців, державних службовців та інших посадових осіб. Водночас, мішенню стають і пересічні громадяни, яких намагаються залучити до шахрайських операцій або отримати доступ до їхніх фінансових ресурсів. Зловмисники часто використовують контексти, пов'язані із соціальними виплатами, гуманітарною допомогою чи безпековими повідомленнями від імені державних установ, що значно ускладнює виявлення підробки [6].

Як свідчить аналіз практики, серед найпоширеніших сценаріїв фішингу в Україні можна виокремити: 1) підроблені повідомлення від банків про «блокування рахунку» або «оновлення даних клієнта» [7];

2) шахрайські листи з пропозиціями гуманітарної допомоги, соціальних виплат чи компенсацій від імені державних органів [8];

3) спроби викрадення облікових даних військовослужбовців або службових акаунтів державних організацій з метою подальшого поширення дезінформації або шпигунства [9].

Наступним способом викрадення персональних даних, який ми хочемо охарактеризувати, є смішинг – одна з різновидностей фішингових атак, що здійснюється через SMS-повідомлення. Зважаючи на стрімке зростання використання мобільних пристроїв, цей метод набуває все більшої популярності серед кіберзлочинців. Його ключова особливість полягає у тому, що жертва отримує текстове повідомлення, яке містить посилання на шкідливі ресурси або запит на надання конфіденційних даних [10].

Ми переконані, що проблема смішингу в Україні має свої специфічні особливості, які обумовлені як загальним рівнем цифровізації суспільства, так і впливом військового конфлікту. З 2022 року значна частина смішингових атак спрямована на отримання фінансових даних громадян під виглядом повідомлень про соціальні виплати, компенсації або допомогу від держави чи міжнародних організацій. Також поширеною є схема із псевдоповідомленнями від військових адміністрацій про мобілізацію або зміну військового статусу [11, с. 388].

Серед найбільш розповсюджених сценаріїв смішингу в Україні можна виокремити: 1) шахрайські SMS від банківських установ – повідомлення про нібито «блокування картки» чи «підозрілі транзакції», що містять посилання для «підтвердження особи»; 2) псевдоповідомлення про державну допомогу – громадяни отримують SMS від імені соціальних служб, де їх закликають вказати банківські реквізити для нібито отримання грошових виплат; 3) SMS про мобілізацію або повістку: у повідомленні зазначається необхідність з'явитися у військкомат чи підтвердити свою присутність через онлайн-форму, що є пасткою для збору особистих даних.

Наступним способом незаконного заволодіння персональними даними, який ми розглянемо, є атаки через Wi-Fi-мережі. Використання незахищених бездротових підключень є серйозною загрозою для інформаційної безпеки, особливо у місцях масового скупчення людей, де широко використовуються публічні Wi-Fi-точки доступу. Ми переконані, що основна небезпека таких атак полягає у невидимості для користувачів: більшість людей підключаються до безкоштовних мереж, не замислюючись про потенційні ризики [12].

Зловмисники можуть реалізовувати атаки через Wi-Fi-мережі двома основними способами: створенням підроблених мереж так звана – Evil Twin Attack, коли шахраї розгортають точку доступу з ідентичним або дуже схожим ім'ям на офіційну Wi-Fi-мережу кафе, аеропорту, готелю чи торгового центру, змушуючи користувачів передавати всі свої дані безпосередньо зловмиснику, та перехопленням трафіку у незахищених мережах – Man-in-the-Middle Attack, MitM, що передбачає використання

уразливостей незашифрованих з'єднань для отримання логінів, паролів, електронної пошти та фінансових операцій жертви [13, с. 61].

На нашу думку, проблема атак через Wi-Fi-мережі в Україні є особливо актуальною у великих містах, де публічний бездротовий інтернет став невід'ємною частиною повсякденного життя. Використання підроблених точок доступу та експлуатація незахищених мереж дедалі частіше стає інструментом кіберзлочинців, які прагнуть отримати доступ до конфіденційної інформації громадян. Зловмисники активно застосовують методи маніпулювання, створюючи фальшиві Wi-Fi-мережі з назвами на кшталт "Free Airport Wi-Fi", "Kyiv_Cafe_Free" або "Gov-UA Public Wi-Fi", що змушує користувачів несвідомо передавати свої дані. Окрім цього, у місцях масового скупчення людей, таких як готелі, торгові центри чи ресторани, нерідко відбуваються атаки, спрямовані на перехоплення незашифрованого трафіку, що особливо небезпечно для користувачів, які здійснюють банківські операції або вводять паролі без додаткового захисту, наприклад VPN.

Водночас, ми переконані, що особливої гостроти проблема атак через Wi-Fi-мережі набула в Україні в умовах воєнного стану, особливо у прифронтових регіонах, де ризики кіберзагроз суттєво зростають. За відсутності належних заходів щодо підвищення рівня кібергігієни населення може скластися ситуація, за якої зловмисники активно використовуватимуть фальшиві Wi-Fi-мережі для отримання конфіденційної інформації, зокрема даних про військових, переміщення цивільного населення або критичну інфраструктуру. Ми вважаємо, що для мінімізації таких загроз необхідно не лише посилювати заходи безпеки на рівні державних та комерційних установ, а й активно працювати над підвищенням цифрової грамотності громадян. Особливо важливо навчити користувачів розпізнавати потенційно небезпечні підключення та уникати використання незахищених мереж у зонах підвищеного ризику.

Ще одним способом незаконного заволодіння персональними даними, який ми розглянемо, є шкідливе програмне забезпечення (malware) – багатофункціональний інструмент, що активно використовується кіберзлочинцями для збору, викрадення та експлуатації конфіденційної інформації. Його ключова небезпека полягає у прихованому проникненні в систему користувача, що дозволяє зловмисникам здійснювати контроль над пристроєм без відома власника [14].

Ми переконані, що проблема поширення шкідливого програмного забезпечення в Україні потребує особливої уваги, оскільки кібератаки дедалі частіше спрямовані не лише на фінансові установи та комерційні структури, а й на державні органи, військових, журналістів та пересічних громадян. У сучасних умовах особливу загрозу становлять цільові атаки, коли зловмисники використовують спеціально розроблене ПЗ для шпигунства, збору конфіденційної інформації або компрометації важливих даних. Такі атаки можуть мати як економічні, так і безпекові наслідки, адже у разі отримання доступу до чутливих відомостей зловмисники можуть використовувати їх для маніпулювання, вимагання або дестабілізації ситуації в країні [15].

Останнім способом викрадення персональних даних, який ми хотіли б проаналізувати, є загрози, пов'язані з використанням соціальних мереж та мобільних застосунків. Ми переконані, що соціальні платформи, які стали ключовим елементом цифрового простору, одночасно є потужним джерелом ризиків, пов'язаних із розголошенням конфіденційної інформації. Користувачі, добровільно публікуючи особисті дані, місце перебування, професійну діяльність, родинні зв'язки та інші чутливі відомості, можуть навіть не підозрювати, що ці дані можуть бути використані зловмисниками для створення фішингових атак, соціальної інженерії чи навіть фінансового шахрайства. Особливо небезпечними є випадки, коли зловмисники збирають інформацію з відкритих профілів, створюючи детальні цифрові портрети жертв, що значно полегшує здійснення персоналізованих атак [16, с. 66].

Не менш серйозною загрозою є мобільні застосунки, які можуть слугувати інструментом збору персональних даних без усвідомленої згоди користувача. Особливо ризикованими є додатки, що завантажуються зі сторонніх ресурсів або навіть деякі програми, доступні в офіційних магазинах, які запитують надмірні дозволи, включаючи доступ до контактної книги, геолокації, камери, мікрофона, фото та фінансової інформації. У багатьох випадках користувачі, не перевіряючи достовірність запитів, автоматично надають ці дозволи, що дозволяє зловмисникам збирати, аналізувати та використовувати отримані дані у шахрайських або шпигунських цілях. Окрему загрозу становлять програми, що приховано здійснюють пересилання даних на віддалені сервери, продаючи інформацію третім особам або використовуючи її для цільової реклами, соціального маніпулювання чи фінансового шахрайства.

Висновки

Проблема незаконного заволодіння персональними даними набуває критичного значення в умовах стрімкого розвитку цифрових технологій та загострення глобальних кіберзагроз. Ми переконані, що зростання кількості кіберзлочинів, особливо в умовах військових конфліктів та інформаційних війн, вимагає системного та багаторівневого підходу до їх запобігання. Удосконалення кримінального законодавства, посилення міжнародного співробітництва у сфері кібербезпеки, впровадження ефективних механізмів державного контролю та моніторингу кіберзагроз – ці заходи є необхідними для створення ефективної системи захисту персональних даних. Водночас ми вважаємо, що критично важливим аспектом є підвищення цифрової грамотності населення, оскільки без обізнаності громадян навіть найсучасніші технології кіберзахисту можуть бути малоефективними. Лише консолідовані зусилля держави, бізнесу та суспільства здатні мінімізувати ризики несанкціонованого доступу до персональних даних та забезпечити належний рівень інформаційної безпеки.

На додаток, суттєву роль у боротьбі з викликами цифрової епохи відіграє розвиток інноваційних технологій моніторингу та протидії кіберзлочинам, зокрема систем на основі штучного інтелекту. Використання таких рішень дозволяє оперативно ідентифікувати загрози, аналізувати поведінкові моделі атак, прогнозувати можливі вразливості та запобігати витоку персональних даних. Проте ми вважаємо, що жоден технологічний інструмент не замінить необхідності формування культури кібергігієни серед користувачів. Усвідомлене ставлення до цифрової безпеки, дотримання базових правил захисту персональних даних та критичне сприйняття інформації є ключовими факторами у запобіганні кіберзагрозам. Лише завдяки комплексному підходу, який поєднує технологічні, правові та освітні заходи, можливо створити безпечне цифрове середовище, яке відповідатиме викликам сучасності та гарантуватиме ефективний захист персональних даних.

Список використаних джерел

1. 90+ Cyber Crime Statistics 2025: Cost, Industries & Trends. Astra: website. URL: https://www.getastra.com/blog/security-audit/cyber-crime-statistics/
2. IBM Cost of a Data Breach Report 2023 – вартість витоків даних сягнула рекордного максимуму. *IO guards: веб-сайт*. URL: https://10guards.com/ua/blog/2024/01/07/ibm-cost-of-a-data-breach-report-2023-reveals-huge-business-data-breach-costs/
3. The Latest 2025 Cyber Crime Statistics (updated January 2025). AAG: website. URL: https://aag-it.com/the-latest-cyber-crime-statistics/
4. Названа кількість кібератак в Україні за минулий рік. *Слово і діло*: веб-сайт. URL: https://www.slovoidilo.ua/2024/01/31/novyna/suspilstvo/nazvana-kilkist-kiberatak-ukrayini-mynulyj-rik

5. Гринько Л.П. Фішинг як спосіб вчиення шахрайства у мережі інтернет. Полтавський правовий часопис. 2022. № 4. DOI: https://doi.org/10.21564/2786-7811.4.287956
6. Кіберполіція попереджає про шахрайство під виглядом соціальних виплат. Міністерство внутрішніх справ: вебсайт. URL: https://mvs.gov.ua/uk/news/kiberpoliciya-poperedzaje-pro-saxraistvo-pid-viglyadom-socialnix-viplat
7. Фішинговий сайт: що це, ознаки, як убезпечити свої платежі. Zen: website. URL: https://www.zen.com/uk/blog/personal-finance-uk/phishing-site-what-are-the-signs-how-to-secure-your-payments/
8. Гуманітарна допомога та шахрайство. KPMG: website. URL: https://kpmg.com/ua/uk/blogs/home/posts/2023/01/humanitarna-dopomoha-ta-shakhraystvo-shcho-potribno-znaty-biznesu.html
9. Фішинг — одна з технік, що використовують російські хакери для атак на Україну — Держспецзв'язку. Армія inform: вебсайт. URL: https://armyinform.com.ua/2023/03/17/fishyng-ekspluatacziya-tehnichnyh-vrazlyvostej-ta-shpz-osnovni-metody-rosijskyh-hakeriv-u-drugomu-pivrichchi-2022/
10. Akanbi Caleb. Phishing and Smishing Attacks. URL: https://www.researchgate.net/publication/381583123_Phishing_and_Smishing_Attacks
11. Саєнко М.І. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. Науковий вісник Ужгородського Національного Університету. Серія Право. 2021. № 64. С. 386-391
12. Чому Wi-Fi в громадських місцях може бути небезпечним для персональних даних. Informator.ua: вебсайт. URL: https://informator.ua/uk/chomu-wi-fi-v-gromadskih-miscyah-mozhe-buti-nebezpechnim-dlya-personalnih-danih
13. İ. Kara, "Twin Ghosts: Evil Twin Attacks in Wireless Networks and Defense Mechanisms", Bitlis Eren University Journal of Science and Technology, vol. 14, no. 2, pp. 58–74, 2024, doi: 10.17678/beuscitech.1450756.
14. Dumitrasc, V., Serral-Gracià, R. (2024). User Behavior Analysis for Malware Detection. In: Katsikas, S., et al. Computer Security. ESORICS 2023 International Workshops. ESORICS 2023. Lecture Notes in Computer Science, vol 14399. Springer, Cham. https://doi.org/10.1007/978-3-031-54129-2_6
15. Безпека в інтернеті: кіберполіція інформує про види комп'ютерних вірусів. Офіційний сайт кіберполіції України: вебсайт. URL: https://cyberpolice.gov.ua/article/bezpeka-v-interneti-kiberpolicziya-informuye-pro-vydy-kompyuternyx-virusiv-5886/
16. Мельник К.С. Обробка та захист персональних даних в соціальних мережах. Інформація і право. 2014. № 3 (12). С. 64-69