

УДК 004.056.53:355Ю271(477)

[https://doi.org/10.52058/2786-6025-2024-2\(30\)-867-884](https://doi.org/10.52058/2786-6025-2024-2(30)-867-884)

Лучик Світлана Дмитрівна доктор економічних наук, професор, професор кафедри протидії кіберзлочинності, Харківський національний університет внутрішніх справ, м. Кам'янець-Подільський, 32307, тел.: (097) 788-34-70, <https://orcid.org/0000-0003-0757-1140>

Лучик Василь Єфремович доктор економічних наук, професор, професор кафедри протидії кіберзлочинності, Харківський національний університет внутрішніх справ, м. Кам'янець-Подільський, 32307, тел.: (068) 445-97-67, <https://orcid.org/0000-0002-1997-0272>

ЗАХИСТ ТА КІБЕРБЕЗПЕКА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В УКРАЇНІ В УМОВАХ ВІЙНИ

Анотація. Стаття присвячена дослідженню проблем захисту інтелектуальної власності від кіберзагроз та ризиків, які набули особливого значення та актуальності в умовах розв'язаної в Україні повномасштабної війни. Багато компаній зіштовхуються з підвищеним ризиком втрати цінної інтелектуальної власності або зриву досліджень і розробок через витік даних.

Досліджено українські тенденції в сфері інтелектуальної власності за 2019-2023 роки (за 9 місяців). Зокрема, проаналізовано динаміку надходження заявок та реєстрації об'єктів промислової власності, авторських та суміжних прав. Особлива увага приділена здобуткам в сфері інтелектуальної власності у роки повномасштабної війни.

Авторами акцентовано увагу на кримінальній відповідальності, яка передбачена вітчизняним законодавством за порушення прав на об'єкти інтелектуальної власності, особливо з використанням комп'ютерної техніки. Проаналізовано різні види кіберзлочинів, які спрямовуються на сферу інтелектуальної власності. Серед них фішингові атаки, інсайдерські атаки, промислове шпигунство, кіберпереслідування, порушення авторських прав тощо.

В статті досліджені основні законодавчі документи щодо захисту прав на об'єкти інтелектуальної власності в Україні, які набули чинності під час воєнного стану. Підкреслена необхідність суворого дотримання чинного законодавства щодо збереження комерційних таємниць, захисту винаходів, торгових знаків, авторських прав з метою необхідності посиленого інноваційного розвитку та інвестиційної привабливості держави в умовах повоєнної економіки.

Запропоновані рекомендації щодо запровадження ефективної політики захисту об'єктів інтелектуальної власності в українських компаніях з метою посилення їх інформаційної безпеки, стійкості та конкурентоспроможності.

Ключові слова: інформаційна безпека, кібербезпека, інтелектуальна власність, право на об'єкт інформаційної власності, кіберзагроза, кіберзлочин, захист.

Luchyk Svitlana Dmytrivna Doctor of Economics, Professor, Professor of the Department of Combating Cybercrime, Kharkiv National University of Internal Affairs, Kamianets-Podilskyi, 32307, tel.: (097) 788-34-70, <https://orcid.org/0000-0003-0757-1140>

Luchyk Vasyl Yefremovych Doctor of Economics, Professor, Professor of the Department of Combating Cybercrime, Kharkiv National University of Internal Affairs, Khmelnytskyi, 32307, tel.: (068) 445-97-67, <https://orcid.org/0000-0002-1997-0272>

DEFENCE AND CYBERSECURITY OF INTELLECTUAL PROPERTY IN UKRAINE DURING THE WAR

Abstract. The article is devoted to the study of the problems of defending intellectual property from cyber threats and risks, which have become especially important and relevant in the context of the full-scale war unleashed in Ukraine. Many companies face an increased risk of losing valuable intellectual property or disrupting research and development due to data breaches.

The article examines Ukrainian trends in the field of intellectual property for 2019-2023 (for 9 months). In particular, the dynamics of applications and registration of industrial property, copyright and related rights is analyzed. Particular attention is paid to the achievements in the field of intellectual property during the years of full-scale war.

The authors emphasize the criminal liability provided for by national legislation for infringement of intellectual property rights, especially with the use of computer equipment. The author analyzes various types of cybercrime aimed at the intellectual property sphere. These include phishing attacks, insider attacks, industrial espionage, cyber harassment, copyright infringement, etc.

The article analyzes the main legislative documents on defence of intellectual property rights in Ukraine which came into force during martial law. The author emphasizes the need for strict compliance with the current legislation on the preservation of trade secrets, protection of inventions, trademarks, and copyrights in order to enhance the innovative development and investment attractiveness of the state in the post-war economy.

The author offers recommendations for implementing an effective policy of intellectual property protection in Ukrainian companies in order to strengthen their information security, sustainability and competitiveness.

Keywords: information security, cybersecurity, intellectual property, right to an object of information property, cyber threat, cyber crime, defence.

Постановка проблеми. Питання забезпечення інформаційної безпеки та кібербезпеки в Україні в умовах повномасштабної війни з РФ стали питаннями виживання української держави. Ворог постійно атакує органи державної влади, медіаресурси, енергетичну сферу та сферу логістики. За даними Державної служби спеціального зв'язку та захисту інформації під час війни кількість ворожих кібератак зросла втричі. [1]. Однак, все частіше об'єктами кібератак стають бізнес-компанії. Відбуваються витoki інформації, мають місце електронне шахрайство, зломи комерційних структур тощо. Багато компаній зіштовхуються з підвищеним ризиком втрати цінної інтелектуальної власності або зриву досліджень і розробок через витік даних.

Отже, перед українською державою постали виклики захисту інформації у різних сферах, в тому числі в сфері інтелектуальної власності.

Аналіз останніх досліджень і публікацій. В умовах війни питання забезпечення високого рівня інформаційної безпеки та кібербезпеки в різних сферах людської діяльності набули особливого значення та актуальності. Ряд науковців, таких як Аніщук В.В. [2], Левченко О.В., Охрімчук В.В. [3], Карпаченков М.П., Тулупов В.В. [4], Рибальченко Л.В. [5] розглядали ці питання в контексті посягання кіберзлочинів проти основ національної безпеки України. Дослідженню сучасного стану вітчизняного ринку інтелектуальної власності, а також питанням правового захисту об'єктів інтелектуальної власності в умовах воєнного стану присвятили свої праці Кронда О.Ю., Зосименко О.М. [6], Чуницька І.І., Бондарчук О.С. [7], Боярчук О.М. [8], Галупова Л.І. [9], Шаповалова А.О., Запотоцька О.В., Гуржій А.В. [10].

Мета статті – дослідження основних проблем, пов'язаних із посиленням кіберзагроз та ризиків об'єктам інтелектуальної власності під час воєнного стану, а також висвітлення заходів, які необхідно застосовувати для забезпечення їх захисту та безпеки.

Виклад основного матеріалу. У «Загальній декларації прав людини» (1948 р.) визначається, що кожна людина має право на свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів [11]. Інформація, як результат інтелектуальної діяльності людини, може існувати як самостійний об'єкт, так і у формі результатів творчості, що охороняються системою права інтелектуальної власності. Останнє визначається як право особи на результат інтелектуальної, творчої діяльності або на інший об'єкт права інтелектуальної

власності і закріплено ст. 418 Цивільного кодексу України [12]. Право на інтелектуальну власність може належати окремим фізичним та юридичним особам, групам фізичних осіб та державі. Інтелектуальна власність охоплює права на винаходи, авторські твори, торгові марки, інші інтелектуальні надбання та відіграє важливу роль у захисті інновацій, творчості та конкурентоспроможності національних та міжнародних рівнів. З розвитком технологій, зокрема, цифрових, та удосконалення методів та засобів виробництва значно збільшився асортимент та різновид товарів, які є носіями поняття «інтелектуальна власність».

Дослідження динаміки надходжень заявок на об'єкти промислової власності за 2010-2023 роки однозначно підтвердили, що воєнні конфлікти в Україні негативно вплинули на розвиток творчості, іноваційності, креативності в суспільстві. Так, якщо у 2010 р. до Держдепартаменту надійшло 46260 заявок на об'єкти промислової власності, то у 2014 р. в умовах розв'язаної війни на Донбасі, їх кількість скоротилась до 44387, а з початком повномасштабної війни у 2022 р. число заявок скоротилось до 28971 одиниць. У 2022 році до Національного органу інтелектуальної власності (НОІВ) було подано близько 2,4 тис. заявок на корисні моделі, понад 2,7 тис. - на винаходи, 819 – на промислові зразки, 23014 – на торговельні марки (з них 16095 – за національною процедурою). Практично аналогічна ситуація з авторськими правами на твір. Якщо у 2019 р. Укрпатентом було прийнято і розглянуто 11076 заявок на реєстрацію авторського права на твір, у 2021 р. – 9158 заявок, то протягом 2022 року на державну реєстрацію авторського права на твір надійшло лише 5739 заявок. Здійснено 4882 державні реєстрації на твір, видано 6346 свідоцтв. Якщо порівняти з 2021 роком, то кількість державних реєстрацій авторського права на твір зменшилась на 53,3% [13].

Однак, незважаючи на ті складні умови війни, в яких перебуває Україна: втрата людських ресурсів, руйнування та знищення будівель, обладнання, переміщення підприємств, наукових та освітянських установ з зони бойових дій в інші регіони країни, сфера інтелектуальної власності все ж такі поступово починає відновлюватись. За 9 місяців 2023 року відбулося відчутне збільшення (на 44,1%) кількості надходження заявок на об'єкти промислової власності (ОПВ) порівняно з 2022 роком (рис. 1). Відбулось це переважно за рахунок збільшення числа заявок на торговельні марки (за національною процедурою) на 50,4%, та на корисні моделі – на 46,8%. Якщо порівняти показники 9 місяців 2019 та 2023 років, то тут побачимо, наскільки суттєво зменшились цифри. Так, загальна кількість поданих заявок на ОПВ зменшилась практично на 40%. Відбулось це переважно за рахунок зменшення числа заявок на корисні моделі (на 78,7%) та промислові зразки (на 57,1%).

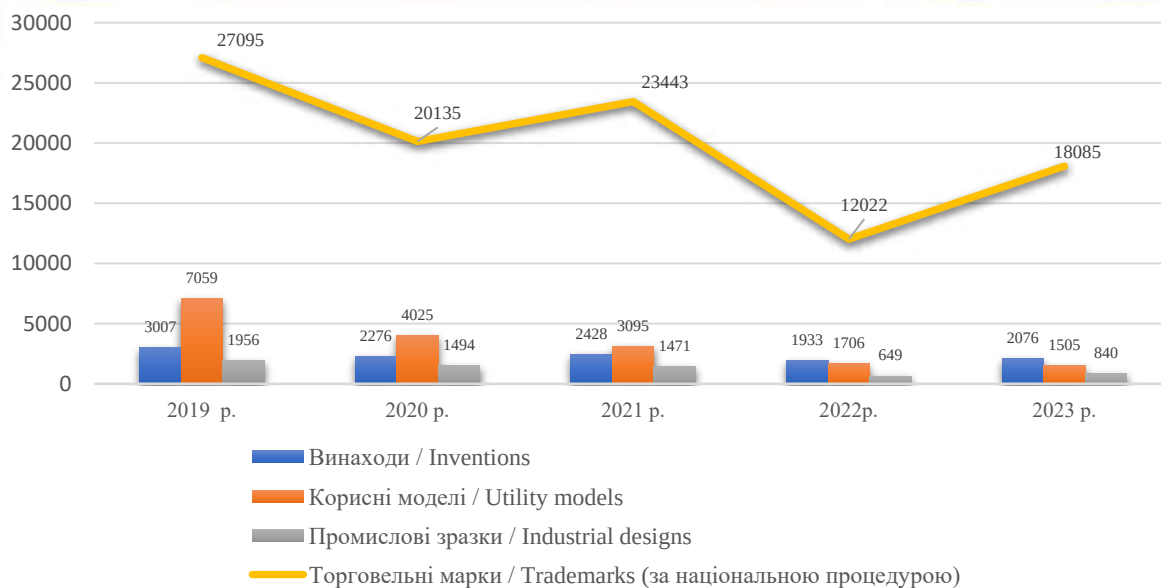


Рис. 1. Надходження заявок на об'єкти промислової власності в Україні, поданих у 2019-2023 роках (за 9 місяців)
Джерело: [14].

Якщо проаналізувати статистику реєстрації об'єктів промислової власності в Україні за цей же період (рис. 2), то тут ситуація дещо інша. Впродовж дев'яти місяців 2023 року здійснено близько 13,8 тис. реєстрацій на ОПВ, зокрема, 914 реєстрацій винаходів. Це на 33,4% менше за показник аналогічного періоду попереднього 2022 року, однак частка реєстрацій винаходів на ім'я іноземних заявників збільшилась на 3,3%, що становить 63,2% від загальної кількості. Також спостерігається невеликий приріст у кількості реєстрацій корисних моделей – на 1,9%, порівняно з кількістю реєстрацій за аналогічний період 2022 року. Було видано більш ніж 1,8 тис. патентів на корисні моделі, з них 98,6% на ім'я національних заявників. Також за цей період було здійснено реєстрацію 450 промислових зразків, при цьому кількість реєстрацій на ім'я іноземних заявників практично не змінилась порівняно з аналогічним періодом минулого року. Що стосується реєстрації торговельних марок за національною процедурою, то за 9 місяців 2023 року їх кількість склала більш ніж 10,5 тис. одиниць. Серед них понад 80% реєструються торговельні марки на ім'я національних заявників.

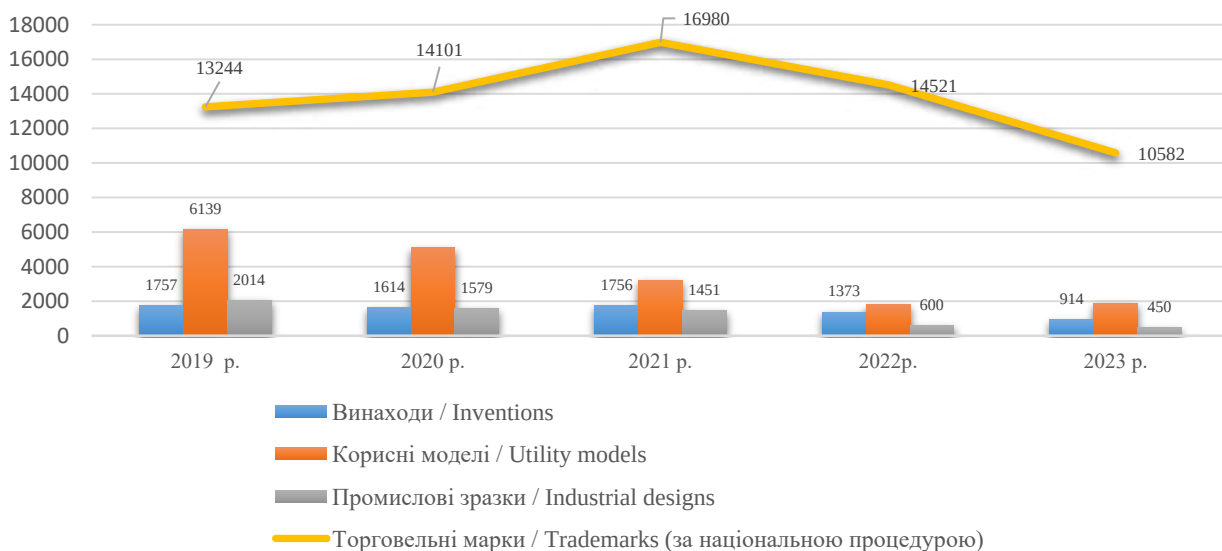


Рис. 2. Реєстрація об'єктів промислової власності в Україні у 2019-2023 роках (за 9 місяців)
Джерело: [14].

У 2022 р. число заявок на авторське право на твір скоротилось порівняно з 2019 р. на 40,8%, на службовий твір – на 67,3%, кількість договорів про передання (відчуження) майнових прав на твір зменшилась на 40,0%, про передачу права на використання твору – на 82,6% (табл. 1). У 2023 р. ситуація з реєстрацією авторських прав значно покращилась. Протягом 9 місяців 2023 року було подано 6048 заявок для реєстрації авторського права на твір, що на 45,9% більше, ніж у 2022 р. Порівняно з відповідним періодом попереднього року, кількість заявок на авторське право на службовий твір збільшилась на 124,3%, кількість договорів, що стосуються права автора на твір – на 74,1%, договорів про передачу права на використання твору – на 325,0%.

Таблиця 1

Динаміка надходжень заявок для реєстрації авторського права та договорів в Україні, що стосуються права автора на твір, поданих у 2019-2023 роках (за 9 місяців)

Показники	2019 р.	2020 р.	2021 р.	2022р.	2023 р.	Відносне відхилення, %		
						2023 р. до 2019 р.	2023 р. до 2022 р.	2022 р. до 2019 р.
Авторське право на твір	7006	4177	6043	4145	6048	-13,7	45,9	-40,8
Авторське право на службовий твір	1121	623	889	367	823	-26,6	124,3	-67,3
Договори про передання (відчуження) майнових прав на твір	482	285	353	166	289	-40,0	74,1	-65,6
Договори про передачу права на використання твору	23	12	14	4	17	-26,1	325,0	-82,6

Джерело: [14].

Зрозуміло, що Україні потрібно і далі намагатись відновлювати сферу інтелектуальної власності, посилювати інноваційність її підприємств, стимулювати економічне зростання та створювати робочі місця. Особливо важливим завданням в цьому напрямку є посилення захисту інтелектуальної власності.

В Україні за порушення прав на об'єкти інтелектуальної власності передбачена кримінальна відповідальність згідно ст.ст. 176, 177, 229 Кримінального кодексу України та адміністративна відповідальність, що закріплено в статтях 51-2, 164-3, 164-6, 164-7, 164-9, 164-13, 345 Кодексу України про адміністративні правопорушення. Санкції цих статей передбачають такі види адміністративних стягнень, як штраф та конфіскація об'єкта адміністративного правопорушення. І В.М. Фурашев стверджує [15], що майже всі зловживання крім, плагіату, у сфері створення (формування) об'єкту права інтелектуальної власності з використанням сучасних програмно-інструментальних та телекомунікаційних засобів зводяться до кіберзлочинності, а точніше – до несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, або до несанкціонованого збуту, або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, або до несанкціонованих дій з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

Дійсно, сьогодні комп'ютерні загрози створюють значні ризики для збереження комерційних таємниць, винаходів, торгових знаків, авторських прав тощо. Так, якщо за оцінками John Patrick Gelinne, Don Fancher, Emily Mossburg, об'єкти інтелектуальної власності для окремої компанії можуть становити до 80% її вартості, то будь-яка успішна кібератака, яка призводить до крадіжки IP-адреси, може просто зруйнувати бізнес [16]. За оцінками фахівців, у США індустрії з інтенсивним використанням інтелектуальної власності сьогодні забезпечують понад 45 мільйонів робочих місць і крадіжка інтелектуальної власності обходиться економіці США в 600 мільярдів доларів на рік, що свідчить про масштабність проблеми [17].

Виділяють такі основні властивості кіберзлочинів [18] як:

інтелектуальний характер, тобто здійснення кіберзлочину вимагає певного набору знань;

доступність здійснення кіберзлочину людьми невисоких соціальних і вікових можливостей;

анонімність і неперсоніфікованість кіберзлочинів;

висока латентність кіберзлочинності;

віддаленість кіберзлочинців від жертв;

значне зростання кількості кіберзлочинів, що пов'язане зі все більшим розповсюдженням Інтернету в різних сферах і здешевлення Інтернет-послуг.

За даними відкритої платформи Opendatabot за вісім місяців 2023 року в Україні було відкрито майже 60 000 кримінальних проваджень за шахрайство за статтею 190 ККУ. Це найбільший показник за останні роки: 2021 р. – 23847 кримінальні справи, 2022 р. – 32086. Однак лише 14% від цих справ у січні-серпні 2023 році доходило до суду, що вдвічі менше, ніж у 2021 році (30%) [19].

Серед кіберзлочинів, які посягають на права інтелектуальної власності, слід виділити фішинг, кіберпереслідування, шахрайство, кіберзалякування, спам, порушення даних щодо комерційних таємниць, авторських прав, торгівельних марок.

Сучасний фішинг є одним із найпоширеніших методів викрадення облікових даних. Кіберзлочинці використовують різні методи, які обманним шляхом змушують співробітників компаній надавати доступ до особистих або корпоративних даних, наприклад, паролів або номерів кредитних карток. Для цього вони використовують електронну пошту, текстові повідомлення та телефонні дзвінки. За допомогою фішингу зловмисники доставляють вірусні програми в ІТ-системи компанії. Протягом 2022 року кількість російських спроб фішингу проти України зросла на 250%. Найбільш потужні кібератаки були здійснені в перші чотири місяці 2022 року. Основною їх ціллю стали понад 150 державних установ і головною мішенню було Міністерство оборони України. Після здійснення фішингових атак, російські хакери використовували шкідливе програмне забезпечення "wiper", за допомогою якого намагалися стерти критичні дані [20]. Основним методом боротьби з фішингом є кібергігієна співробітників.

Інформаційна безпека, і, зокрема, кібербезпека відіграють неабияку роль у забезпеченні довіри та лояльності клієнтів до компаній в епоху цифрових технологій. Споживачі очікують, що їх персональні дані будуть надійно захищені компаніями під час використання технічних продуктів і послуг. І будь-яке порушення даних може зруйнувати ту багаторічну довіру, яку компанія вибудувала зі своїми клієнтами. Проте, досить часто кіберзлочинці зламують корпоративну мережу компанії з метою отримати доступ до конфіденційної інформації, пов'язаної з IP-адресами, щоб, наприклад, отримати списки клієнтів, їх особисті дані. Паттарафан Пайбун стверджує, що оскільки компанії все частіше використовують взаємозв'язок між своїми пристроями у процесі цифровій трансформації, особливо при оцифруванні цінної корпоративної інформації та інтелектуальної власності, що використовується в бізнесі, то уразливість до кіберзагроз в них постійно зростає. А коли

комерційні таємниці компанії розкриваються громадськості, то вони вже не вважаються комерційними таємницями. І компанія може втратити свою вартість, конкурентоспроможність і переваги» [21].

Звичайно, що зі зростанням обізнаності суспільства про існуючі кіберзагрози та ризики, споживачі, ймовірно, вимагатимуть ще більш надійного захисту своїх даних. Таким чином, компанії, які інвестуватимуть у кібербезпеку та зможуть продемонструвати високий рівень захисту інформації про клієнтів, з більшою ймовірністю отримають конкурентну перевагу та збережуть лояльність клієнтів.

Одним з проявів комп'ютерної злочинності є порушення авторських прав, що включає несанкціоноване використання, створення та розповсюдження копій програмного забезпечення, несанкціонований продаж і незаконне копіювання інформації з веб-сайтів або блогів за допомогою незаконних дій, таких як посилання та фрейми. Посилання (лінкінг, гіперлінкінг) забезпечує розміщення у структурі вебсайту елементів програмного коду, які дають можливість перейти на сторінку іншого вебсайту або переглядати її вміст без переходу на цю сторінку. В залежності від способу вбудови посилання в «тіло» сайту, є такі різновиди лінкінгу як звичайний лінкінг (розміщення на сайті гіперпосилання на стартову сторінку іншого вебсайту) та дїп лінкінг (розміщення гіперпосилання на будь-яку сторінку іншого вебсайту, крім стартової). До різновидів лінкінгу відносять ембедінг або інлайн лінкінг, який забезпечує включення частини коду іншої сторінки таким чином, що окремий об'єкт іншої сторінки (зображення, відео) відображається без потреби переходу на інший сайт. А також фреймінг («framing»), який включає цілі сторінки інших вебсайтів в окремі «фрейми» (секції), які не перетинаються між собою. Отже, при використанні посилань HTTP протокол не бачить відмінності між дїп лінками, як не бачить різниці і між звичайним лінком та дїплінком, оскільки технічно всі лінки є рівними. Однак такий підхід вводить в оману, що ці два веб-сайти, наприклад, мають однаковий домен і право власності. Також дозволяє переглядати контент без перегляду реклами на сайті [22]. Фреймінг дозволяє користувачам лише отримувати доступ до захищеного авторським правом вмісту веб-сайту в браузері, який використовує користувач. Проте фреймери не несуть відповідальності за відтворення, передачу чи розповсюдження вмісту, захищеного авторським правом.

Значну шкоду безпеці інформації компанії наносять так звані інсайдерські атаки. Інсайдерськими вважають спрямовані дії мотивованих суб'єктів, які мають легітимний доступ до інформаційних активів та навички для здобуття цінної інформації, знають уразливі місця інформаційних систем і бізнес-процесів, для завдання матеріальних збитків та/або репутаційних втрат організації [23]. Такими мотивованими суб'єктами є працівники,

колишні працівники, ділові партнери компанії. Дії інсайдерів можуть носити як злісний, навмисний, так і ненавмисний характер, тому їх важко передбачити і знешкодити. Через це фахівці оцінюють інсайдерські загрози як унікальний виклик для кібербезпеки, хоча за даними CERT Insider Threat Center, 75% інсайдерських дій залишаються непоміченими [24]. Інсайдери мають набагато більше можливостей, ніж сторонні зловмисники, оскільки вони мають розширений доступ до систем і даних організації, щоб виконувати свою роботу. Також інсайдери в переважній більшості ознайомлені із заходами та процедурами безпеки свого роботодавця та можуть їх обійти. Відповідно до звіту ESET про витоки даних за 2023 рік, 19% із приблизно 5200 витоків даних були спричинені діями персоналу. У іншому дослідженні за 2022 рік кількість цих подій перевищила 6800, а організації витратили близько 15,4 мільйона доларів на рік на усунення наслідків. [25].

Дослідження персональних даних та проведення постійного моніторингу та аналізу дій персоналу дасть можливість керівництву компаній уникнути багатьох кіберінцидентів. Запровадження системи управління доступом на основі ролей зможе допомогти обмежити доступ працівникам до конфіденційних даних і систем, за винятком тільки тих, яким він потрібен для виконання службових обов'язків. Обов'язково потрібно проводити перевірку репутації підрядників і постачальників перед наданням їм доступу до конфіденційних даних.

Інформація компанії, що закрита від публічного доступу, може стати об'єктом для промислового шпигунства, яке може здійснюватися різними шляхами. Це прихована фото- та відеозйомка, прослуховування розмов, перехоплення комп'ютерної інформації, підкуп працівника із застосуванням технічних засобів, представлених у вигляді спеціально розроблених програмних продуктів для розкрадання електронних даних, а також апаратних пристроїв для зняття акустичної та візуальної інформації. Промислове шпигунство є недешевим способом крадіжки даних. Наприклад, середня вартість комплексу заходів зі збору закритих даних про невелику компанію і її співробітників знаходиться в межах 2.000 – 3.000 дол.США. Установка апаратури знімання інформації в одному кабінеті – 400 – 600 дол. США [26]. Нелегальне проникнення в інформаційні системи і мережі компаній тягне за собою не лише фінансові збитки, а й псування репутації.

Серйозною проблемою для компаній, які працюють зі споживачами, може стати кіберсквотинг. Цей кіберзлочин полягає у реєстрації, використанні та пропонуванні до продажу доменного імені із несумлінним наміром отримати прибуток від паразитування на гудвілі або торговельній марці, яка належить іншій особі. Для реалізації своїх злочинних намірів зловмисники можуть отримувати SSL сертифікат для своїх шахрайських доменів, щоб здати їх більш автентичними та важко розпізнаваними. Кіберзлочинці можуть

орендувати сервери та хостинг для розміщення шахрайських веб-сайтів, що робить їх менш вразливими до блокування і сприяє подовженню тривалості атак. Всі ці дії можуть заподіяти серйозні збитки і підірвати ділову репутацію.

Розвиток та значне поширення інформаційно-комунікаційних технологій в сучасному суспільстві розширили можливості кіберзлочинців в напряму залякування, ображання, приниження людей або групи людей, що, в свою чергу, створює загрози їх психологічній та соціальній безпеці. Агресивна поведінка злочинців у віртуальному просторі розцінюється як кіберпереслідування, кіберцькування та кібервбивство. Психологічні кібератаки призводять до сильних емоційних переживань людей, зниження їх самооцінки, підвищують репутаційні ризики (завдають шкоди іміджу та репутації), руйнують та послаблюють реальні соціальні зв'язки, навіть створює небезпеку для життя. Із-за особливостей віртуального середовища кіберзлочинці не можуть адекватно оцінювати шкоду, заподіяну ними жертві через кіберпростір, оскільки психологічно сприймають взаємодію з жертвою як з цифровим об'єктом, а не з реальною людиною. Для агресивного психологічного впливу на особистість у кіберпросторі використовуються мобільний зв'язок, месенджери, електронна пошта, форуми, соціальні мережі, web-камери, сервіси відеохостингу тощо [27, с.41-42].

Отже, повномасштабна війна в Україні прискорила перехід компаній до цифрової трансформації, змусила значну частину працівників працювати у віддаленому режимі роботи з використанням хмарних технологій, підвищила роль інтелектуальної власності в успіху продукту. Однак, всі ці процеси супроводжуються збільшенням інцидентів, пов'язаних з несанкціонованим доступом злочинців до конфіденційної інформації, витоком цінних даних, порушенням прав інтелектуальної власності. Для посилення рівня інформаційної та кібербезпеки організацій, захисту їх інтелектуальної власності від порушень або загрози порушень під час воєнного стану українською державою приймається ряд законодавчих документів. Так, 01.12.2022 року був прийнятий Закон України «Про внесення змін до Кодексу України про адміністративні правопорушення, Кримінального кодексу України та Кримінального процесуального кодексу України щодо відповідальності за порушення авторського права і (або) суміжних прав» [28]. Закон передбачає внесення відповідних змін щодо санкцій за порушення авторських прав, зокрема:

вилучення положень щодо адміністративної та кримінальної відповідальності в контексті маркування контрольними марками примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних;

посилення адміністративної та кримінальної відповідальності за порушення авторського права і суміжних прав;

криміналізація нових форм вчинення злочинів щодо авторських та суміжних прав, тобто внесення нової статті до Кримінального Кодексу

України – ст. 176-1 «Фінансування порушення авторського права і суміжних прав», а також доповнення до ст. 176 КК України «Порушення авторського права і суміжних прав», що передбачають розширення кримінально караних форм вчинення цього злочину.

З 15 квітня 2023 року в Україні набув чинності Закон «Про внесення змін до деяких законодавчих актів України щодо посилення захисту прав інтелектуальної власності», яким внесено важливі зміни, які дозволять правовласникам більш ефективно захищати свої права в судовому порядку [29]. Зміни спрямовані на посилення захисту прав інтелектуальної власності, які дозволять правовласникам застосовувати додаткові інструменти в боротьбі з контрафактом та спростять стягнення компенсації з порушників. Правовласник в судовому порядку має право витребувати інформацію про походження і мережі розповсюдження товарів або надання послуг, що порушують право інтелектуальної власності. Таку інформацію може бути витребувано в порушника, імпортера, продавця, виробника та будь-яких інших осіб, задіяних в ланцюгу виготовлення та розповсюдження товарів чи послуг з порушенням прав інтелектуальної власності. Замість стягнення збитків, правовласники відтепер мають право вимагати стягнення з порушників компенсації за порушення прав інтелектуальної власності на промислові зразки (зареєстровані та незареєстровані), торговельні марки, винаходи і корисні моделі, компонування напівпровідникових виробів. Компенсація має становити не менше ніж розмір ліцензійного платежу, і може бути визначена судом в більшому розмірі, залежно від обсягу порушення, вини порушника та інших обставин, що мають істотне значення.

15 серпня 2023 року Кабінет Міністрів України вніс зміни до своєї Постанови «Про затвердження Порядку сплати зборів за дії, пов'язані з охороною прав на об'єкти інтелектуальної власності» від 23 грудня 2004 р. № 1716 [30]. Постановою передбачено застосування нових зборів, які мають розблокувати механізм post-grant opposition для винаходів, корисних моделей та промислових зразків. Передбачено збільшення розміру знижки до 25% за подання заявок на торговельні марки в електронній формі. Тобто, мінімальний розмір збору за подання заявки одним заявником для одного класу товарів чи послуг у чорно-білому виконанні відтепер складатиме 3000 гривень. Суттєво збільшилась вартість зборів за звернення до Апеляційної палати НОІВ.

Висновки. Таким чином, за 2023 рік Україна, попри виклики повномасштабної війни, за останній рік Україна змогла завершити реформу у сфері інтелектуальної власності, що важливо як для євроінтеграції України, так і для інноваційного розвитку та інвестиційної привабливості держави. В контексті набуття Україною статусу кандидата в члени ЄС інтелектуальна власність та інновації мають визначальну роль. На думку Ю. Свириденко, першого віце-прем'єр-міністра України – міністра економіки «гармонізуючи

правила та процедури у цих сферах, ми не лише відкриваємо Україну світові, як інноваційну та креативну націю, а й істотно покращуємо її інвестиційну привабливість. І від того, наскільки ми будемо у цьому ефективними, великою мірою залежатиме інноваційна повоєнна відбудова України” [31].

Отже, загрози інформаційній безпеці та кібербезпеці організацій є постійною загрозою для їх об’єктів інтелектуальної власності. З метою забезпечення зниження ризиків, слід розробити і дотримуватись комплексної та ефективної політики захисту і безпеки інтелектуальної власності:

комплексно підходити до захисту комп’ютерних систем і мереж, використовуючи засоби багатофакторної автентифікації та технологію захищеного входу, захисту корпоративної пошти, кінцевих точок IT-інфраструктури, віртуальні приватні мережі (VPN);

запровадити систему управління доступом персоналу до конфіденційної інформації з розподілом прав доступу, постійним моніторингом дій персоналу, регулярною перевіркою журналів доступу;

застосовувати надійне шифрування конфіденційних даних, пов’язаних з інтелектуальною власністю, щоб захистити їх від несанкціонованого перегляду, перехоплення;

регулярне навчання персоналу з питань правового захисту та кібербезпеки об’єктів інтелектуальної власності;

перевірка репутації співробітників, підрядників, постачальників перед наданням їм доступу до конфіденційних даних.

Література:

1. Інформаційна безпека в умовах війни. Досвід Metinvest Діджитал. *Metinvest Digital*. URL: <https://metinvest.digital/ua/page/information-security-in-conditions-war> (дата звернення: 06.01.2023).
2. Аніщук В. Інформаційна безпека як об’єкт посягання злочинів проти основ національної безпеки України. *Науковий вісник Ужгородського національного університету*, 2023, Том 2 № 77. Серія: Право. С.139-140. DOI: <https://doi.org/10.24144/2307-3322.2023.77.2.23>
3. Левченко О.В., Охрімчук В.В. Особливості антиукраїнського інформаційного (кібер) впливу на Україну. *Захист інформації*. 2022. Т. 24, № 4. С. 156-163.
4. Карпеченков, М. П., Тулупов В.В. Кібербезпека в умовах війни: що, хто, як. Застосування інформаційних технологій у правоохоронній діяльності: матеріали Круглого столу (м. Харків, 14 груд. 2022 р.) / МВС України, Харк. нац. ун-т внутр. справ, Ф-т № 6, Каф. кібербезпеки та DATA-технологій. Харків: ХНУВС, 2022. С. 104-108.
5. Рибальченко, Л.В. Кіберзлочинність у глобальному просторі. *Наук. вісн. Дніпропетр. держ. ун-ту внутр. справ*. 2022. Спецвип. № 2 (121): Держава і право України в умовах воєнного стану. С. 524-530.
6. Кронда О.Ю., Зосименко О.М. Інтелектуальна власність в Україні в умовах воєнного стану. *Електронне наукове видання «Аналітично-порівняльне правознавство»*, 2022, №4. С.104-108. DOI: <https://doi.org/10.24144/2788-6018.2022.04.19>
7. Чуницька І.І., Бондарук О.С. Сучасний стан ринку інтелектуальної власності в Україні. *Економіка та суспільство*, 2023, №52. DOI: <https://doi.org/10.32782/2524-0072/2023-52-55>

8. Боярчук О.М. Захист права інтелектуальної власності: особливості здійснення в Україні, США та країнах Європейського союзу (Німеччина, Франція). *Електронне наукове видання «Аналітично-порівняльне правознавство»*, 2023, №6. С.184-188. DOI <https://doi.org/10.24144/2788-6018.2023.06.32>

9. Галупова Л. І. Захист прав інтелектуальної власності в умовах воєнного стану. Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2022. Т. 2. С. 745-749.

10. Шаповалова А.О., Запотоцька О.В., Гуржій А.В. Правовий захист об'єктів інтелектуальної власності в умовах воєнного стану: збереження та безпека інновацій. *Юридичний науковий електронний журнал*, 2023, №2. С.642-645. DOI <https://doi.org/10.32782/2524-0374/2023-2/153>

11. Загальна декларація прав людини. Документ від 10.12.1948 №995_015. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 08.01.2024).

12. Цивільний Кодекс України. Кодекс від 16.01.2003 № 435-IV. *Відомості Верховної Ради України (ВВР)*, 2003, №№ 40-44, ст.356. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text> (дата звернення: 08.01.2024).

13. Річний звіт НОІВ 2022 рік. *Український національний офіс інтелектуальної власності та інновацій*. URL: <https://ukrpatent.org/uk/articles/UKRNOIVI-statistics> (дата звернення: 10.01.2024).

14. Інтелектуальна власність у цифрах. Показники діяльності у сфері інтелектуальної власності за 9 місяців 2023 року. УКРНОІВІ. Київ: 2023. 36 с.

15. Фурашев В. М. Проблеми забезпечення права на об'єкт інтелектуальної власності в умовах кібербезпеки. *Кібербезпека та інтелектуальна власність: проблеми правового забезпечення*: Матеріали міжнародної науково-практичної конференції. 21 квітня 2017 р., м. Київ, в 2-х частинах.. Частина перша. / Упоряд. : В. М. Фурашев, С. Ю. Петряєв. Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2017. С. 25-30.

16. The hidden costs of an IP breach: Cyber theft and the loss of intellectual property by John Patrick Gelinne, Don Fancher, Emily Mossburg. *Deloitte InSights*. URL: <https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html/#endnote-1> (дата звернення: 12.01.2024).

17. IP Commission 2021 Review Updated Recommendations March 2021. The IP Commission. URL: https://www.nbr.org/wp-content/uploads/pdfs/publications/ip_commission_2021_recommendations_mar2021.pdf (дата звернення: 12.01.2024).

18. Кримінальна відповідальність за кіберзлочини. *WikiLegalAid. Безоплатна правова допомога*. URL: https://wiki.legalaid.gov.ua/index.php/Кримінальна_відповідальність_за_кіберзлочини (дата звернення: 14.01.2024).

19. Кількість справ про шахрайство у 2023 році сягнула історичного антирекорду. *Опендатабот*. URL: <https://opendatabot.ua/analytics/fraud-pandemic-2> (дата звернення: 15.01.2024).

20. Небезпека фішинг-листів та як захистити бізнес. *Економічна правда*. URL: <https://www.epravda.com.ua/columns/2023/06/29/701729/> (дата звернення: 15.01.2024).

21. Загрози кібербезпеці в IP: на що слід звернути увагу у 2023 році. *AsiaIP. Informed Analyses*. URL: <https://asiaiplaw.com/section/in-depth/cybersecurity-threats-in-ip-what-to-watch-for-in-2023> (дата звернення: 16.01.2024).

22. Поставив лінк і порушив авторське право? Розповідають юристи Axon Partners. AIN.ua. URL: <https://ain.ua/ru/2021/05/06/vsmisli-postaviv-link-i-porushiv-avtorske-pravo/> (дата звернення: 16.01.2024).

23. Шевченко С.М., Жданова Ю.Д., Складаний П.М., Бойко С.В. Інсайтери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність. Кібербезпека: освіта, наук, техніка, 2022, №3(15), с.175-185.

24. Kontrolle und Disziplinen або як позбавитися інсайдерських загроз. IT Solutions. URL: <https://it-solutions.ua/blog/kontrolle-und-disziplinen-abo-yak-pozbavitsya-insajderskih-zagrozo/> (дата звернення: 17.01.2024).

25. Небезпека ближче, ніж ви думаєте: як компанії захиститися від інсайдерських загроз. ESET. URL: <https://www.eset.com/ua/about/newsroom/blog/business-security/nebezpeka-blyzhche-nizh-vy-vvazhayete-yak-kompaniyi-zakhystytsya-vid-insayderskykh-zahroz/> (дата звернення: 17.01.2024).

26. Промислове шпигунство. Міфи і реальність. IAC. Search For Invisible. URL: <https://iac.com.ua/uk/news/promislove-shpigunstvo-mifi-i-realni/> (дата звернення: 18.01.2024).

27. Турбан В. В., Сердюк Л. З., Москаленко В. В. Соціокультурні детермінанти розвитку психології особистості в Україні: монографія; за наук. ред. В. В. Турбан. Київ: Інститут психології імені Г. С. Костюка НАПН України, 2023, с.41-42.

28. Про внесення змін до Кодексу України про адміністративні правопорушення, Кримінального кодексу України та Кримінального процесуального кодексу України щодо відповідальності за порушення авторського права і (або) суміжних прав: Закон України від 01.12.2023 №2803-IX. URL: <https://zakon.rada.gov.ua/laws/show/2803-20#Text> (дата звернення: 18.01.2024).

29. Про внесення змін до деяких законодавчих актів України щодо посилення захисту прав інтелектуальної власності : Закон України від 20.03.2023 №2974-IX. URL: <https://zakon.rada.gov.ua/laws/show/2974-20#Text> (дата звернення: 19.01.2024).

30. Про внесення змін до Порядку сплати зборів за дії, пов'язані з охороною прав на об'єкти інтелектуальної власності: Постанова Кабінету міністрів України від 15 серпня 2023 р. №859. URL: <https://zakon.rada.gov.ua/laws/show/859-2023-%D0%BF#n2> (дата звернення: 20.01.2024).

31. За останній рік Україна змогла завершити реформу у сфері інтелектуальної власності, що важливо для євроінтеграції, – Свириденко. LB.ua. URL: https://lb.ua/economics/2023/10/24/580983_ostanniy_rik_ukraina_zmogla.htm (дата звернення: 20.01.2024).

References:

1. Informatsiina bezpeka v umovakh viiny. Dosvid Metinvest Didzhytal. [Information security in wartime. Metinvest Digital's experience]. *Metinvest Digital*. Retrieved from: <https://metinvest.digital/ua/page/information-security-in-conditions-war>

2. Anishchuk, V. (2023). Informatsiina bezpeka yak ob'iekt posiahannia zlochyniv proty osnov natsionalnoi bezpeky Ukrainy [Information security as an object of offences against the foundations of national security of Ukraine]. *Scientific Bulletin of Uzhhorod National University*, vol.2, 77, 139-140. [in Ukrainian]. <https://doi.org/10.24144/2307-3322.2023.77.2.23>

3. Levchenko, O.V. & Okhrimchuk, V.V. (2022). Osoblyvosti antyukrainskoho informatsiinoho (kiber) vplyvu na Ukrainu [Features of anti-Ukrainian information (cyber) influence on Ukraine]. *Information protection*, vol.24, 4, 156-163.

4. Karpechenkov, M.P. & Tulupov, V.V. (2022). Kiberbezpeka v umovakh viiny: shcho, khto, yak [Cybersecurity in wartime: what, who, how]. Kruhlyi stil "Zastosuvannia informatsiinykh tekhnolohii u pravookhoronnii diialnosti" - Round table discussion "The use of information technology in law enforcement: materials of the round table" (pp.104-108). Kharkiv: Kharkiv National University of Internal Affairs. [in Ukrainian].

5. Rybalchenko, L.V. (2022). Kiberzlochynnist u hlobalnomu prostori [Cybercrime in global space]. *Nauk. visn. Dnipropetr. derzh. un-tu vnutr. sprav. - Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*, special issue, 2(121), 524-530. [in Ukrainian].

6. Kronda, O.Yu. & Zosimenko, O.M. (2022). Intelktualna vlasnist v Ukraini v umovakh voiennoho stanu [Intellectual property in Ukraine under martial law]. *Elektronne naukove vydannia «Analitichno-porivnialne pravoznavstvo» - Electronic scientific publication "Analytical and comparative jurisprudence"*, 4, 104-108. <https://doi.org/10.24144/2788-6018.2022.04.19> [in Ukrainian].

7. Chynytska, I.I. & Bondaruk, O.S. (2023). Suchasnyi stan rynku intelektualnoi vlasnosti v Ukraini [The current state of the intellectual property market in Ukraine]. *Ekonomika ta suspilstvo - Economy and Society*, 52. <https://doi.org/10.32782/2524-0072/2023-52-55> [in Ukrainian].

8. Boyarchuk, O.M. (2023). Zakhyst prava intelektualnoi vlasnosti: osoblyvosti zdiisnennia v Ukraini, SShA ta krainakh Yevropeiskoho soiuzu (Nimechchyna, Frantsiia) [Protection of intellectual property rights: peculiarities of implementation in Ukraine, the USA and the countries of the European Union (Germany, France)]. *Elektronne naukove vydannia «Analitichno-porivnialne pravoznavstvo» - Electronic scientific publication "Analytical and comparative jurisprudence"*, 6, 184-188. <https://doi.org/10.24144/2788-6018.2023.06.32> [in Ukrainian].

9. Galupova, L. I. (2022). Zakhyst prav intelektualnoi vlasnosti v umovakh voiennoho stanu. [Protection of intellectual property rights under martial law]. *Mizhnarodna naukov0-praktychna konferentsiia "Yevropeyskyi vybir Ukrainy, rozvytok nauky ta natsionalna bezpeka v realiakh masshtabnoi viiskovoi ahresii ta hlobalnykh vyklykiv KhKhI stolittia» - International scientific and practical conference "The European choice of Ukraine, the development of science and national security in the realities of large-scale military aggression and global challenges of the 21st century"*, vol.2, (pp. 745-749). Odesa: "Helvetyka" Publishing House. [in Ukrainian].

10. Shapovalova, A.O., Zapototska, O.V. & Gurzhii, A.V. (2023). Pravovyi zakhyst obektiv intelektualnoi vlasnosti v umovakh voiennoho stanu: zberezhennta ta bezpeka innovatsii [Legal protection of intellectual property objects under martial law: preservation and safety of innovations]. *Yurydychnyi naukovyi elektronnyi zhurnal - Legal scientific electronic journal*, 2, 642-645. <https://doi.org/10.32782/2524-0374/2023-2/153> [in Ukrainian].

11. Universal Declaration of Human Rights. (1948, December 10). *Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of Verkhovna Rada of Ukraine*. Retrieved from: https://zakon.rada.gov.ua/laws/show/995_015#Text [in Ukrainian].

12. Tsyvilnyi Kodeks Ukraine [Civil Code Ukraine]. (2003, January 16). *Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of Verkhovna Rada of Ukraine*. Retrieved from: <https://zakon.rada.gov.ua/laws/show/435-15#Text> [in Ukrainian].

13. *Richnyi zvit NOIV 2022 rik. Ukrainyskyi natsionalnyi ofis intelektualnoi vlasnosti ta innovatsii* [Annual report of NOIP 2022. Ukrainian National Office of Intellectual Property and Innovation] (2023). Retrieved from: <https://ukrpatent.org/uk/articles/UKRNOIVI-statistics> [in Ukrainian].

14. *Intelktualna vlasnist u tsyfrakh. Pokaznyky diialnosti u sferi intelektualnoi vlasnosti za 9 misiatsiv 2023 roku. [Intellectual property in numbers. Indicators of activity in the field of intellectual property for 9 months of 2023]* (2023). Kyiv: IP OFFICE. 36 p.

15. Furashev, V. M. (2017). Problemy zabezpechennia prava na ob'ekt intelektualnoi vlasnosti v umovakh kiberbezpeky [Problems of ensuring the right to an object of intellectual property in the conditions of cyber security]. *Mizhnarodna naukov0-praktychna konferentsiia "Kiberbezpeka ta intelektualna vlasnist: problemy pravovoho zabezpechennia" - International scientific and practical conference "Cyber security and intellectual property: problems of legal support"* (pp. 25-30). Kyiv: National Technical University of Ukraine "Kyiv Polytechnic Institute named after Ihor Sikorsky" Edition "Polytechnic" [in Ukrainian].

16. Gelinne J. P., Fancher D., Mossburg E. (2016). The hidden costs of an IP breach: Cyber theft and the loss of intellectual property. *Deloitte InSights*. Retrieved from: <https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html/#endnote-1> [in English].

17. IP Commission 2021 Review Updated Recommendations March 2021. The IP Commission. Retrieved from: https://www.nbr.org/wp-content/uploads/pdfs/publications/ip_commission_2021_recommendations_mar2021.pdf [in English].

18. Kryminalna vidpovidalnist za kiberzlochyny [Criminal liability for cybercrimes] (n.d.). WikiLegalAid. *Bezoplatna pravova dopomoha - Free legal assistance*. Retrieved from: https://wiki.legalaid.gov.ua/index.php/Кримінальна_відповідальність_за_кіберзлочини [in Ukrainian].

19. Killist sprav pro shakhraistvo u 2023 rotsi shahnula istorychnoho antyrekordu [The number of fraud cases in 2023 reached a historical anti-record] (2023). *Opendatabot*. Retrieved from: <https://opendatabot.ua/analytics/fraud-pandemic-2> [in Ukrainian].

20. Nebezpeka fishynh-lystiv ta yak zakhystyty biznes [The danger of phishing lists and how to protect your business] (2023). *Ekonomichna pravda*. Retrieved from: <https://www.epravda.com.ua/columns/2023/06/29/701729/> [in Ukrainian].

21. Zahrozy kiberbezpeti v IP: na shcho slid zvernuty uvahu u 2023 rotsi [Cyber Security Threats in IP: What to Watch for in 2023] (2023). *AsiaIP. Informed Analyses*. Retrieved from: <https://asiaiplaw.com/section/in-depth/cybersecurity-threats-in-ip-what-to-watch-for-in-2023> [in Ukrainian].

22. Postavyv link i porushyv avtorske pravo? Rozpovidaiut yurysty Axon Partners. [Did you post a link and violate copyright? The lawyers of Axon Partners talk]. *AIN.ua*. Retrieved from: <https://ain.ua/ru/2021/05/06/vsmisli-postaviv-link-i-porushiv-avtorske-pravo/> [in Ukrainian].

23. Shevchenko, S.M., Zhdanova, Yu.D., Skladanyi, P.M. & Boiko S.V. (2022). Insaidery ta insaiderska informatsiia: sut, zahrozy, diialnist ta pravova vidpovidalnist [Insiders and insider information: nature, threats, activities and legal liability]. *Kiberbezpeka: osvita, nauk, tekhnika - Cyber security: education, science, technology*, 3(15), 175-185. [in Ukrainian].

24. Kontrolle und Disziplinen abo yak pozbavytysia insaiderskykh zahroz [Kontrolle und Disziplinen or how to get rid of insider threats.]. *IT Solutions*. Retrieved from: <https://it-solutions.ua/blog/kontrolle-und-disziplinen-abo-yak-pozbavitysia-insajderskih-zagroz/> [in Ukrainian].

25. Nebezpeka blyzhche, nizh vy dumaiete: yak kompanii zakhystytysia vid insaiderskykh zahroz [Danger is closer than you think: How companies can protect themselves from insider threats]. *ESET*. Retrieved from: <https://www.eset.com/ua/about/newsroom/blog/business-security/nebezpeka-blyzhche-nizh-vy-vvazhayete-yak-kompaniyi-zakhystytysia-vid-insajderskykh-zagroz/> [in Ukrainian].

26. Promyslove shpyhunstvo. Mify i realnist [Industrial espionage. Myths and reality]. *IAC. Search For Invisible*. Retrieved from: <https://iac.com.ua/uk/news/promislove-shpigunstvo-mifi-i-realni/> [in Ukrainian].

27. Turban, V. V., Serdyuk, L. Z. & Moskalenko, V. V. (2023). Sotsio-kulturni determinanty rozvytku psykholohii osobystosti v Ukraini [Socio-cultural determinants of the development of personality psychology in Ukraine]: monograph; for sciences ed. V. V. Turban. (pp. 41-42). Kyiv: H. S. Kostyuk Institute of Psychology of the National Academy of Sciences of Ukraine.

28. Zakon Ukrainy Pro vnesennia zmin do Kodeksu Ukrainy pro administratyvni pravoporushennia, Kryminalnoho kodeksu Ukrainy ta Kryminalnoho protsesualnoho kodeksu Ukrainy shchodo vidpovidalnosti za porushennia avtorskoho prava i (abo) sumizhnykh prav : pryiniaty 1 grud. 2023 roku №2803-IX. [Law of Ukraine On amendments to the Code of Ukraine on Administrative Offenses, the Criminal Code of Ukraine and the Criminal Procedure Code of Ukraine regarding liability for copyright infringement and (or) related rights from December 1 2023 №2803-IX]. Retrieved from: <https://zakon.rada.gov.ua/laws/show/2803-20#Text> [in Ukrainian].

29. Закон України Про внесення змін до деяких законодавчих актів України щодо посилення захисту прав інтелектуальної власності : прийнятий 20 бер. 2023 року №2974-IX. [Law of Ukraine On making changes to some legislative acts of Ukraine regarding strengthening the protection of intellectual property rights from March 20 2023 №2974-IX]. Retrieved from: <https://zakon.rada.gov.ua/laws/show/2974-20#Text> [in Ukrainian].

30. Постанова Кабінету міністрів України Про внесення змін до Порядку сплати зборів за дії, пов'язані з окhoronoю прав на об'єкти інтелектуальної власності : прийнята 15 серп. 2023 року №859 [Resolution of the Cabinet of Ministers of Ukraine On making changes to some legislative acts of Ukraine regarding strengthening the protection of intellectual property rights from August 15 2023 №859]. Retrieved from: <https://zakon.rada.gov.ua/laws/show/859-2023-%D0%BF#n2> [in Ukrainian].

31. За останній рік Україна змогла завершити реформу у сфері інтелектуальної власності, що важливо для євроінтеграції, – Свиріденко [Over the past year, Ukraine was able to complete the reform in the field of intellectual property, which is important for European integration, - Sviridenko] (2023). LB.ua. Retrieved from: https://lb.ua/economics/2023/10/24/580983_ostanniy_rik_ukraina_zmogla.htm [in Ukrainian].