УДК 339.166: 347.77
DOI: https://doi.org/10.32782/2224-6282/190-45

Корнілова І.М.
кандидат економічних наук, доцент,
доцент кафедри менеджменту інноваційної та інвестиційної діяльності,
Київський національний університет імені Тараса Шевченка
ORCID: https://orcid.org/0000-0003-0715-5825

Kornilova Iryna
Taras Shevchenko National University of Kyiv

КІБЕРПРОМИСЛОВЕ ШПИГУНСТВО: СУТНІСТЬ ТА НАСЛІДКИ

У статті висвітлюються теоретичні аспекти кіберпромислового шпигунства. Обґрунтовується значення захисту комерційної таємниці компаній від кібервторгнень, що підтверджується розмірами збитків від них у світовому економічному просторі. Розглядається сутність кіберпромислового шпигунства через призму його співставлення з кібершпигунством та промисловим шпигунством. Встановлюється, що кіберпромислове шпигунство є різновидом кібершпигунства та промислового шпигунства. Визначаються риси, притаманні кіберпромисловому шпигунству, розкриваються особливості їх прояву у кіберпросторі. Значна увага приділяється виділенню та з'ясуванню змісту можливих негативних для компаній наслідків успішних кібератак, упереджувальне врахування яких при розбудові системи захисту комерційної таємниці сприятиме підвищенню ефективності її використання.

Ключові слова: *інтелектуальна власність, комерційна таємниця, кіберпромислове шпигунство, кібершпигунство, промислове шпигунство, кібератака.*

CYBER-INDUSTRIAL ESPIONAGE: ITS NATURE AND CONSEQUENCES

The article highlights the theoretical aspects of cyber-industrial espionage. The importance of ensuring the protection of trade secrets of companies from cyber intrusions is substantiated, which is confirmed by the amount of damage caused by successful cyber attacks on the scale of the global economic space. The paper examines the essence of cyber industrial espionage through the prism of its comparison with cyber espionage and industrial espionage. It is established that cyber-industrial espionage is a type of cyber-espionage and industrial espionage. Its key features are illegality, unethicality, and unauthorised access by an unauthorised user to a company's trade secret in cyberspace, which is carried out in favour of private entities in order to gain competitive advantages and economic benefits. By the logic of the dialectical combination of the general and the particular, the author identifies the features inherent in cyber-industrial espionage (in particular, its covert, highly organised, planned, systematic nature; wide arsenal of possible technologies, methods of implementation, their combined use; a significant scope and list of negative consequences, difficulties in assessing losses from cyber intrusions, etc.), and reveals the peculiarities of their manifestation in cyberspace. Considerable attention is paid to identifying and clarifying the content of possible negative consequences of successful cyberattacks for companies, including financial losses associated with the theft of confidential information; reputational losses due to loss of trust in the company; theft of intellectual property, R&D results kept as commercial secrets; disruption of critical business processes of companies; forced changes in business practices to improve security, legal, regulatory, psychological and emotional consequences. Determination of the essential characteristics of cyber-industrial espionage and the range of possible negative consequences of its implementation is of theoretical and methodological importance for the development of an effective system of trade secret protection in companies and will help to increase the efficiency of its use.

Keywords: *intellectual property, trade secrets, cyber-industrial espionage, cyber-espionage, industrial espionage, cyber-attack.*

JEL classification: *O34, K42, L14, L86*

Постановка проблеми. Зростання усвідомлення значення інтелектуальної власності як джерела досягнення системи цілей сучасних компаній логічно пов'язано зі зростанням конкуренції на ринках високотехнологічної продукції. У розрізі збільшення внеску комерційної таємниці у забезпечення конкурентоспроможності компаній у інноваційному просторі, однією з серйозних загроз їх діяльності залишається промислове шпигунство.

В умовах інтенсивного зростання інформаційної економіки, глобалізації інформаційно-комунікаційних технологій, їх посиленої дифузії в усі галузі економіки та сфери життєдіяльності людини, промислове шпигунство переходить у нову якість, все більше набуваючи формату кіберпромислового шпигунства. Розвиток індустрії 4.0 (з охопленням до 26 млрд. персональних пристроїв, бізнес- та промислового обладнання [1] створює нові можливості, додатковий майданчик для доступу до конфіденційної інформації, комерційної таємниці конкурентів. Як свідчать аналітичні дані, вже зараз втрати від кіберзлочинності становлять до 0,8 відсотка світового ВВП, або 600 мільярдів доларів на рік. За оцінками McAfee і Центру стратегічних і міжнародних досліджень (CSIS) щодо економічної вартості кіберзлочинності, у Північній Америці вона становить 0,78% ВВП. При чому, США тільки за рахунок міжнародних хакерських кібератак втрачає до 100 млрд. дол. щороку. В Європі кіберзлочинність має більший економічний вплив, який оцінюється в 0,84% регіонального ВВП [2; 3]. Згідно з дослідженнями PricewaterhouseCoopers [1], у ЄС 91% всіх кібер-інцидентів стосувалися викрадення або спроби викрадення комерційної таємниці. У США, згідно з дослідженням 200 справ щодо викрадення комерційних таємниць, практично всі випадки мали кібер-аспект [4].

За даними опитувань [5], 85% організацій-респондентів зазнали принаймні однієї успішної кібератаки протягом 2020 р., при цьому, програмами-вимагачами були скомпрометовані 73% організацій. Також, результати аналітичних досліджень [6] демонструють зростання динамізму кібершпигунства. Так, за шість років – з 2014 р. по 2020 р. – частка організацій, які були скомпрометовані успішними кібератаками, зросла з 62% до 86%. Також продовжує зростати частка організацій, які платять викуп кіберзлочинцям, зокрема, з 49% у 2018 р. до 72% у 2021 р.

Крім того, слід звернути увагу на загрози, пов'язані з перетворенням кібершпигунства у потужний вид бізнесу та розвитком світового ринку кібершпигунства. Експерти [3] називають кіберзлочинність процвітаючою галуззю, яка надає кіберзлочинцям в межах цієї темної екосистеми широкий спектр послуг, обладнання, інструментів та платформ.

Все це слугує серйозним застережливим індикатором для посилення занепокоєності щодо зростання кіберпромислового шпигунства та його негативних, часто руйнівних, наслідків для комерційної таємниці компаній, інноваційного бізнесу загалом. Означене обумовлює потребу вивчення питань сутності кіберпромислового шпигунства для вироблення компаніями ефективних управлінських рішень щодо протидії його здійсненню.

Аналіз останніх досліджень і публікацій. Проблематика кіберпромислового шпигунства має міждисциплінарний характер, перетинаючись з широким колом питань, пов'язаних із забезпеченням набуття, використання, захисту комерційної таємниці, використання відповідної інформації для отримання конкурентних переваг. Важливими векторами дослідження є питання економічного, промислового шпигунства, організації захисту комерційної таємниці, які вивчаються в працях фахівців, серед яких [7–18]: Г. Андрощук, В. Бадрак, Л. Березіна, Е. Бітті, В. Богданович, Б. Братанов, В. Ван, Е. Гіббс, В.Ч. Істтом, А. Крейн. М.Л. Мюллер, В. Кентон, Г. Малицька, Т. Хоу, Ю. Якубівська та інші дослідники. Проблематику кібербезпеки, кіберпростіру, кібертероризму, кібератак, засобів та заходів захисту від них розглядають К. Бейкер, В. Бурячок, С. Гнатюк, І. Діордіца, Д. Дубов, К. Корсун, Є. Котух, П. Нойман, Дж. О'Харат, В. Толубко, С. Толюпа, Дж. Франкенфілд, В. Хорошко, Ю. Якубівська [19–29] та інші дослідники. Водночас, інтенсивний розвиток цифрових мереж, їх активне використання для збільшення результативності комерціалізації об'єктів інтелектуальної власності, посилення їх впливу на рівень конкурентоспроможності інноваційних компаній обумовлює потребу поглибленого вивчення питань кіберпромислового шпигунства.

Метою дослідження є сприяння комплексному розумінню сутності кіберпромислового шпигунства та його наслідків для вироблення ефективних управлінських рішень щодо протидії його здійсненню сучасними інноваційними організаціями.

Методологічним фундаментом досягнення мети є комплексний підхід до розуміння кіберпромислового шпигунства. Досягнення мети наукових розвідок спирається на використання методів: абстрагування, наукової дескрипції, теоретичного узагальнення, індукції й дедукції, порівняння, діалектичного поєднання загального та особливого; декомпозиції та структурування. Використання означених методів сприятиме поглибленому розумінню напрямів формування дієвої системи захисту комерційної таємниці від несанкціонованого використання при динамічному розвитку процесів цифровізації.

Виклад основних результатів дослідження. Підвищення значення інтелектуальної власності у досягненні цілей інноваційних компаній в умовах посилення трендів діджиталізації економіки знаходить відображення у збільшенні присутності об'єктів інтелектуальної власності у глобальному цифровому просторі, частка яких у трафіку цифрових мереж, за існуючими даними [7], становить понад 70%. В структурі портфелю інтелектуальної власності компаній збільшується значення комерційної таємниці, значна частка якої зберігається у хмарі, що обумовлює важливість її захисту від несанкціонованого використання, насамперед, кіберпромислового шпигунства.

При дослідженні кіберпромислового шпигунства важливим при виділенні сутнісних характеристик є методологічний аспект діалектичного поєднання загального та особливого в його розумінні, також, його співставлення з іншими категоріями у площині використання та захисту комерційної таємниці.

Кіберпромислове шпигунство перетинається з певною кількістю категорій. У загальному розумінні кіберпромислове шпигунство є різновидом шпигунства, яке у найбільш широкому трактуванні можна визначити як доступ до конфіденційної інформації без отримання дозволу власника інформації [13].

Також, кіберпромислове шпигунство є підвидом кібершпигунства. У вітчизняному законодавстві, згідно з Законом України «Про основні засади забезпечення кібербезпеки України», кібершпигунство – це шпигунство, що здійснюється у кіберпросторі або з його використанням [30].

У фаховій літературі щодо розуміння кібершпигунства існує широкий спектр різних бачень. Зокрема, воно розглядається як:

– заходи в кіберпросторі, спрямовані на отримання конфіденційної, секретної або просто чутливої для об'єкта атаки інформації [22];

– використання комп'ютерних мереж для отримання незаконного доступу до конфіденційної інформації, зазвичай тієї, що зберігається урядом або іншою організацією [31];

– кібератаки з метою отримання політичної, комерційної та військової інформації [32];

– різновид кібератаки, під час якої неавторизований користувач намагається отримати доступ до конфіденційних або секретних даних або інтелектуальної власності з метою економічної вигоди, конкурентної переваги чи політичних причин [2; 26];

– несанкціоноване отримання інформації з метою отримання особистої, економічної, політичної чи військової переваги, здійснюваний з використанням обходу (злому) систем комп'ютерної безпеки [21];

– форма кібератаки, яка викрадає секретні, конфіденційні дані або інтелектуальну власність, щоб отримати перевагу над конкурентною компанією чи державною установою [33].

Наведені визначення кібершпигунства охоплюють два його різновиди – економічне та промислове кіберш-

пигунство. Економічне (державне) кібершпигунство здійснюється в кіберпросторі за участю та фінансової підтримки державних служб і спрямоване на державні, приватні установи/особи для незаконного отримання комерційної конфіденційної інформації і досягнення економічних, політичних цілей своєї країни.

На відміну від економічного кібершпигунства, кіберпромислове шпигунство – це свідомо незаконне, неетичне, несанкціоноване отримання у кіберпросторі неавторизованим користувачем доступу до комерційної таємниці на користь приватних структур для отримання конкурентних переваг, економічної вигоди. Таке бачення обумовлюється тим, що кіберпромислове шпигунство є різновидом промислового шпигунства. Останнє розглядається як прихований системний процес збору, управління конфіденційною інформацією, що становить комерційну таємницю, який здійснюється окремою особою/організацією з приватною метою її використання для отримання конкурентних переваг/доходу від продажу зацікавленим особам без дозволу власника інформації з порушенням законодавчих та етичних норм [16].

Звісно, кіберпромисловому шпигунству, за логікою діалектичного поєднання загального та особливого, притаманні родинні риси промислового шпигунства, насамперед, це: комерційна спрямованість; незаконний, неетичний, несанкціонований доступ; високоорганізований, спланований, систематичний, прихований характер; широкий арсенал методів та інструментів здійснення, їх комбіноване використання; значний обсяг, спектр та пролонгованість негативних наслідків, складність оцінювання збитків тощо.

Наведені риси промислового шпигунства у кіберпросторі набувають нових форм прояву. Так, кіберпромислове шпигунство використовується не тільки для збору різних видів інформації, що становить комерційну таємницю, зокрема, для набуття конкурентної переваги, отримання фінансової вигоди (у т.ч. кіберзлочинцями), але й для свідомого нанесення різноманітних збитків компанії-конкуренту, зокрема, через системні руйнування в компанії-об'єкті кібератак, пошкодження/знищення даних щодо об'єктів інтелектуальної власності, комерційно цінної ділової інформації, надійного та безпомилкового функціонування ІКТ компанії, інші руйнівні дії, які можуть бути фатальними для бізнесу. В цьому ракурсі кіберпромислове шпигунство може бути проявлено як кіберсаботаж.

Кіберпромисловому шпигунству притаманне глобальне охоплення, що проявляється в більших масштабах, відсутності географічних бар'єрів здійснення. Важливою рисою є універсальний характер. Його об'єктом може бути будь-яка інформація, яка розміщена в кіберпросторі. Найчастіше об'єктами кібератак стають незапатентовані об'єкти інтелектуальної власності, які зберігаються як комерційна таємниця, результати ДіР, різноманітні види ділової конфіденційної інформації (концепція бізнесу, цілі, стратегії, плани, потенційні пропозиції, дані клієнтів, ціноутворення, дані про продажі, структуру платежів тощо). За результатами проведених досліджень [29], у 2020–2021 рр. до галузей за найбільшою кількістю кібератак, включені фінанси, охорона здоров'я, професійна сфера, державне управління та інформація. Нові вразливості для кібератак пов'язані з динамічним поширенням штучного інтелекту (AI) та Інтернету речей (IoT).

Також, кіберпромислове шпигунство, на думку фахівців [32], використовує анонімність, розсіяність, взаємопов'язаність інформаційних мереж, що обумовлює складність доказовості здійснення кіберзлочину. В його арсеналі широкий набір методичного інструментарію, різноманітні можливості правдоподібного обману (зокрема, через соціальну інженерію).

Високий ступінь професіоналізму, організованості безпосередніх суб'єктів кіберпромислового шпигунства (хакерів, їх організацій/груп), які розглядають його як прибутковий бізнес, на фоні недостатнього рівня усвідомлення багатьма компаніями стратегічних наслідків успішних кібератак, знаходить втілення у прихованому характері їх здійснення, доволі тривалому терміні несанкціонованого доступу до конфіденційної інформації компанії-об'єкта. Часто такі компанії навіть не підозрюють про крадіжку своєї комерційної таємниці, що може призвести до серйозних втрат їх конкурентоспроможності, навіть бізнесу. Певною мірою, з цим пов'язана суттєва складність оцінювання розміру збитків, особливо відтермінованих. За оцінками експертів [34], прямі наслідки кіберпромислового шпигунства становлять близько 10% витрат, з якими стикаються компанії, решта 90% витрат пов'язані з непрямими наслідками, які можна достовірно оцінити через 5–6 років після кіберторгнення. Також, слід приймати до уваги нерідкість випадків, коли компанії після виявлення фактів кібератак, свідомо приховують цей факт, побоюючись репутаційних та інших втрат, що може, у свою чергу, опосередковано підтримувати безкарність та відтворювати мотивацію до кіберпромислового шпигунства.

Існує бачення [32], що компанії часто недооцінюють ризики та негативні наслідки кіберпромислового шпигунства, особливо стратегічного характеру, внаслідок, насамперед, своєї необізнаності, що може призвести до серйозних збитків різного формату через нехтування формуванням ефективної системи захисту.

Серед можливих наслідків кібершпигунства для компанії, насамперед, слід виділити наступні [15; 23; 35–39]:

– фінансові втрати для окремих осіб і організацій, пов'язані з викраденням конфіденційної фінансової інформації; проведенням шахрайських операцій, вимогами викупу за розблокування зашифрованих даних; з розслідуванням і пом'якшенням кібератак; з виплатою юридичних зобов'язань та штрафів, відновленням мереж після атак, з падінням ціни акцій. Наприклад, дослідники безпеки Comparitech [38] за результатами вивчення 40 витоків даних з 34 компаній, зареєстрованих на Нью-Йоркській фондовій біржі, встановили, що після атак акції цих компаній в середньому падали на 3,5%;

– збільшення витрат на заходи упереджувального характеру щодо захисту від кіберторгнення, зокрема, на технології та експертизу кібербезпеки, страхові внески, підтримку зв'язків з громадськістю тощо;

– репутаційні збитки окремих осіб/компаній, обумовлені втратою довіри серед акціонерів, клієнтів, партнерів і громадськості внаслідок витоку конфіденційної інформації, можливого блокування інформаційних ресурсів як методу комунікацій з клієнтами, що може призвести до нівелювання можливостей для бізнесу та фінансових втрат. Прикладом [38] може слугу-

вати постраждала від потужної кібератаки у 2013 році компанія-гігант роздрібної торгівлі Target, репутаційні втрати якої оцінювалися у 18,5 мільйонів доларів;

– крадіжка інтелектуальної власності, даних ДіР, що зберігаються як комерційна таємниця, з довгостроковими негативними результатами для компанії щодо її конкурентних переваг, позицій на ринку, реалізації системи цілей функціонування та розвитку;

– зрив критично важливих бізнес-процесів компаній, зокрема, внаслідок збоїв, блокування мереж/систем (наприклад, через зараження комп'ютерних систем зловмисним програмним забезпеченням, яке стирає важливу інформацію, чи встановлення шкідливого коду на сервері, який блокує доступ до вебсайту тощо), що спричинює простої, зниження продуктивності, затримки в наданні послуг, виконанні зобов'язань, отже, призводить до фінансових втрат;

– юридичні та нормативні наслідки у вигляді судових позовів, санкцій, штрафів через недотримання вимог чинного законодавства, зокрема, щодо захисту даних і конфіденційної інформації; невиконання галузевих норм та договірних зобов'язань. Наприклад, згідно з Регламентом ЄС щодо кіберстійкості [36] введені штрафи для постраждалих виробників і дистриб'юторів у розмірі до 15 мільйонів євро або 2,5 відсотка річних продажів, при виявленні прогалин в безпеці пристроїв, про які не було повідомлено та не усунено належним чином;

– вимушена зміна бізнес-практики для підвищення рівня безпеки (наприклад, відмова компанією від певних форматів онлайн-бізнесу з причини побоювання щодо нездатності належним чином захиститися від кібератак);

– психологічні та емоційні наслідки для людей (стрес, тривога, страх та інші негативні емоції), що впливає на результативність людського капіталу компаній.

Експерти [39] відмічають постійне вдосконалення концепції, методичного інструментарію, навичок здійснення кібератак, що потребує систематичного оновлення, розвитку системи захисту від кіберпромислового шпигунства, врахування кращих світових практик, навчання персоналу для підвищення рівня їх компетентності в означеній площині для недопущення/усунення/мінімізації негативних наслідків кібервторгнень.

Висновки. Кіберпромислове шпигунство в умовах високої динамічності процесів діджиталізації, глобального характеру застосування інформаційно-комунікаційних технологій при реалізації системи цілей діяльності компаній перетворюється на серйозну загрозу їх конкурентоспроможності та розвитку як на національному рівні, так і в масштабах світового економічного простору. Особливо велику занепокоєність кібервторгнення викликають у інноваційних компаній в контексті захисту від несанкціонованого доступу/використання портфеля їх комерційної таємниці.

Кіберпромислове шпигунство є складового кібершпигунства, водночас – це різновид промислового шпигунства, отже, містить притаманні ним загальні риси, що має враховуватися компаніями в практиці розбудови системи захисту від кібератак. При розкритті сутності кіберпромислового шпигунства, насамперед, слід акцентувати увагу на незаконність, неетичність, несанкціонованість доступу неавторизованого користувача до комерційної таємниці організацій у кіберпросторі на користь приватних структур для отримання конкурентних переваг, економічної вигоди.

Для забезпечення ефективності прийняття рішень щодо використання та захисту комерційної таємниці, необхідно упереджувально в управлінській практиці зважати на можливі різноманітні негативні наслідки успішних кібервторгнень, які часто мають пролонгований характер. Звісно, це вимагає від компаній певних ресурсних витрат, які є виправданими в контексті недопущення/усунення/мінімізації можливих збитків.

Формування системи захисту від кіберпромислового шпигунства має спиратися на комплексне розуміння можливих технологій, методів його здійснення на засадах оперативного, гнучкого реагування на нові тренди розвитку кібератак, що формує вектори подальших наукових розвідок в означеній площині дослідження.

Список використаних джерел:

1. PricewaterhouseCoopers. The scale and impact of industrial espionage and theft of trade secrets through cyber. European Commission. 2018. URL: https://ec.europa.eu/docsroom/documents/34841/attachments/1/translations/en/renditions/native

2. Civuli A., Luma-Osmani Sh., Rufati E., Arifi G. Cyber espionage consequences as a growing threat. 2022. URL: https://www.researchgate.net/publication/368461675_Cyber_Espionage_Consequences_as_a_Growing_Threat

3. The economic impacts of cyber crime: how it costs us all. 2022. URL: https://mitigatecyber.com/the-economic-impacts-of-cyber-crime-how-it-costs-us-all/

4. Searle, N. The economic and innovation impacts of trade secrets. Intellectual Property Office. 2021. URL: https://www.gov.uk/government/publications/economic-and-innovation-impacts-of-trade-secrets/the-economic-and-innovation-impacts-of-trade-secrets

5. Threat Landscape Developments. 2021 State-Sponsored Cyber Activity. Herjavec Group's. 2021. 14 p. URL: https://eadn-wc01-3468285.nxedge.io/wp-content/uploads/2021/12/State-Sponsored-Cyber-Activity-Report.pdf

6. Cyberthteat Defense Report. URL: https://cyber-edge.com/cdr/

7. *Андрощук* Г. Економічне шпигунство: зростання масштабів і агресивності. Частина 1. *Наука, технології, інновації*. 2018. № 3. С. 39–49. URL: http://dspace.nbuv.gov.ua/handle/123456789/162638

8. Березіна Л.М. Братанов Б.В. Характерні особливості конкурентної розвідки та промислового шпигунства підприємств. *Інтелект XXI.* 2020. № 2. URL: http://www.intellect21.nuft.org.ua/journal/2020/2020_2/3.pdf

9. Богданович В.Ю., Бадрак В.В. Конкурентна розвідка та промислове шпигунство. *Сучасний захист інформації*. 2014. № 1. С. 16–22. URL: http://nbuv.gov.ua/UJRN/szi_2014_1_5

10. Маліцька Г.Г., Кутаренко Н.Я. Промислове шпигунство в контексті економічної злочинності. *Ефективна економіка.* 2019. № 5. URL: http://nbuv.gov.ua/UJRN/efek_2019_5_32

11. Якубівська Ю.Є. Вплив промислового шпигунства на сферу інтелектуальної власності. *Зовнішня торгівля: економіка, фінанси, право.* 2013. № 4 (69). С. 158–162. URL: http://zt.knute.edu.ua/files/2013/4(69)/uazt_2013_4_24.pdf

12. Beattie A. Corporate espionage: fact and fiction. 2022. URL: https://www.investopedia.com/financial-edge/0310/corporate-espionage-fact-and-fiction.aspx

13. Crane A. In the company of spies: when competitive intelligence gathering becomes industrial espionage. *Business Horizons*, 2005. Volume 48 (3), pp. 233–240. DOI: https://doi.org/10.1016/j.bushor.2004.11.005
14. Gibbs E. The new face of corporate espionage and what can be done about. 2022. URL: https://www.securitymagazine.com/articles/98087-the-new-face-of-corporate-espionage-and-what-can-be-done-about-it
15. Easttom C. Industrial Espionage in Cyberspace. Computer Security Fundamentals 5ed. 2023. URL: https://www.pearsonitcertification.com/articles/article.aspx?p=3172433
16. Hou T., Wang V. Industrial espionage - A systematic literature review (SLR). *Computer&Security.* 2020. Volume 98. URL: https://www.sciencedirect.com/science/article/pii/S0167404820302923
17. Kenton W. Industrial Espionage: Definition, Examples, Types, Legality. 2022. URL: https://www.investopedia.com/terms/i/industrial-espionage.asp
18. Mueller R. F. Industrial espionage: what is it, who's involved and what harm can it cause? *Journal Polygraph.* 2001. Volume: 30. P. 47–55. URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/industrial-espionage-what-it-whos-involved-and-what-harm-can-it
19. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект. Львів. 2018. 320 с. URL: https://kr-labs.com.ua/books/Buryachok-Osnovy-info-ta-ciberbezpeky.pdf
20. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації.* 2013. Т. 19, № 2. С. 118–129. URL: http://nbuv.gov.ua/UJRN/bezin_2013_19_2_8
21. Діордіца І.В. Поняття та зміст кібершпигунства. *Наукові праці Національного університету "Одеська юридична академія".* 2020. В. 26. С. 49–55. URL: http://naukovipraci.nuoua.od.ua/arhiv/tom26/9.pdf
22. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ : НІСД, 2014. 328 с. URL: https://niss.gov.ua/sites/default/files/2015-02/Dubov_mon-89e8e.pdf
23. Корсун К. Огляд ринку кібербезпеки України/ Stakeholders' dialogue in the process of Ukraine's integration into the EU Digital Single Market" Project of European Media Platform 2021. URL: https://eump.org/media/2021/ukraine-into-dsm/korsun_ukr.pdf
24. Котух Є.В. Кібербезпека у публічному секторі: монографія. Харків : Колегіум, 2021. 272 с.
25. Якубівська Ю.Є. Цільові атаки в контексті промислового шпигунства. 2014. URL: http://dspace.wunu.edu.ua/jspui/bitstream/316497/1537/1/10_%D1%84%D0%B0%D1%85.pdf
26. Baker K. What is Cyber Espionage? 2023. URL: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/
27. Neumann P. Computer-Related Risk. ACM Press/Addison Wesley, 1995.
28. O'Harat G. Cyber-espionage: a growing threat to the american economy. *Commlaw conspectus.* 2009. Vol. 19. P. 241–275. URL: https://scholarship.law.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1522&context=commlaw
29. Frankenfield J. Cybrsecurity: Meaning, Types of Cyber Attacks, Common Targets. URL: https://www.investopedia.com/terms/c/cybersecurity.asp
30. Закон України «Про основні засади забезпечення кібербезпеки України», від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради (ВВР),* 2017, № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
31. Cyber espionage. ENISA Threat Landscape. 2020. 10 p. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage/@@download/fullReport
32. From Espionage to Cyber Espionage. URL: https://www.cyber-espionage.ch/
33. What is Cyber Espionage? Vmware. URL: http://www.vmware.com/topics/glossary/content/cyber-espionage.html
34. Study on the scale and impact of industrial espionage and theft of trade secrets through cyber. Pwc. 2019. URL: https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf
35. Bigelow J. Sentonas M. The economic impact of cybercrime and cyber espionage. 2014. URL: https://www.securitysolutionsmedia.com/2014/03/11/the-economic-impact-of-cybercrime-and-cyber-espionage/
36. EU Cyber Resilience Act: what to watch out for now. 2023. URL: https://onekey.com/blog/eu-cyber-resilience-act-what-to-watch-out-for-now/
37. Industrial espionage: the threat to global business. URL: https://www.enderi.fr/Industrial-Espionage-The-Threat-to-Global-Business_a1143.html
38. 6 Ways Cybercrime Impacts Business. URL: https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx
39. The impact of cybersecurity threats and cybercrime on businesses. URL: https://www.bitsioinc.com/cybercrime-impact-on-businesses/

References:

1. PricewaterhouseCoopers. (2018)The scale and impact of industrial espionage and theft of trade secrets through cyber. European Commission. Available at: https://ec.europa.eu/docsroom/documents/34841/attachments/1/translations/en/renditions/native
2. Civuli A., Luma-Osmani Sh., Rufati E., Arifi G. (2022) Cyber espionage consequences as a growing threat. Available at: https://www.researchgate.net/publication/368461675_Cyber_Espionage_Consequences_as_a_Growing_Threat
3. The economic impacts of cyber crime: how it costs us all. (2022). Available at: https://mitigatecyber.com/the-economic-impacts-of-cyber-crime-how-it-costs-us-all/
4. Searle, N. (2021) The economic and innovation impacts of trade secrets. Intellectual Property Office. Available at: https://www.gov.uk/government/publications/economic-and-innovation-impacts-of-trade-secrets/the-economic-and-innovation-impacts-of-trade-secrets
5. Threat Landscape Developments. 2021 State-Sponsored Cyber Activity. (2021) Herjavec Group's. 14 p. Available at: https://eadn-wc01-3468285.nxedge.io/wp-content/uploads/2021/12/State-Sponsored-Cyber-Activity-Report.pdf
6. Cyberthteat Defense Report. (n.d.). Available at: https://cyber-edge.com/cdr/
7. *Androshchuk H. (2018). Ekonomichne shpyhunstvo: zrostannia masshtabiv i ahresyvnosti. Chastyna 1. Nauka, tekhnolohii, innovatsii,* no. 3, pp. 39–49. Available at: http://dspace.nbuv.gov.ua/handle/123456789/162638

8. Berezina L. M. Bratanov B. V. (2020) Kharakterni osoblyvosti konkurentnoi rozvidky ta promyslovoho shpyhunstva pidpryiemstv. *Intelekt XXI,* no. 2. Available at: http://www.intellect21.nuft.org.ua/journal/2020/2020_2/3.pdf

9. Bohdanovych V. Yu., Badrak V. V. (2014) Konkurentna rozvidka ta promyslove shpyhunstvo. *Suchasnyi zakhyst informatsii,* no. 1, pp. 16–22. Available at: http://nbuv.gov.ua/UJRN/szi_2014_1_5

10. Malitska H. H., Kutarenko N. Ya. (2019) Promyslove shpyhunstvo v konteksti ekonomichnoi zlochynnosti. *Efektyvna ekonomika,* no. 5. Available at: http://nbuv.gov.ua/UJRN/efek_2019_5_32

11. Yakubivska Yu. (2013) Vplyv promyslovoho shpyhunstva na sferu intelektualnoi vlasnosti. *Zovnishnia torhivlia: ekonomika, finansy, pravo,* no. 4 (69), pp. 158–162. Available at: http://zt.knute.edu.ua/files/2013/4(69)/uazt_2013_4_24.pdf

12. Beattie A. (2022) Corporate espionage: fact and fiction. Available at: https://www.investopedia.com/financial-edge/0310/corporate-espionage-fact-and-fiction.aspx

13. Crane A. (2005) In the company of spies: when competitive intelligence gathering becomes industrial espionage. *Business Horizons*, vol. 48 (3), pp. 233–240. DOI: https://doi.org/10.1016/j.bushor.2004.11.005

14. Gibbs E. (2022) The new face of corporate espionage and what can be done about. Available at: https://www.securitymagazine.com/articles/98087-the-new-face-of-corporate-espionage-and-what-can-be-done-about-it

15. Easttom C. (2023) Industrial Espionage in Cyberspace. Computer Security Fundamentals 5ed. Available at: https://www.pearsonitcertification.com/articles/article.aspx?p=3172433

16. Hou T., Wang V. (2020). Industrial espionage – A systematic literature review (SLR). *Computer&Security,* vol. 98. Available at: https://www.sciencedirect.com/science/article/pii/S0167404820302923

17. Kenton W. (2022) Industrial Espionage: Definition, Examples, Types, Legality. Available at: https://www.investopedia.com/terms/i/industrial-espionage.asp

18. Mueller R. F. (2001) Industrial espionage: what is it, who's involved and what harm can it cause? *Journal Polygraph,* vol. 30, pp. 47–55. Available at: https://www.ojp.gov/ncjrs/virtual-library/abstracts/industrial-espionage-what-it-whos-involved-and-what-harm-can-it

19. Buriachok V. L., Tolubko V. B., Khoroshko V. O., Toliupa S. V. (2018) Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt. Lviv. 320 p. Available at: https://kr-labs.com.ua/books/Buryachok-Osnovy-info-ta-ciberbezpeky.pdf

20. Hnatiuk S. (2013) Kiberteroryzm: istoriia rozvytku, suchasni tendentsii ta kontrzakhody. *Bezpeka informatsii*, vol. 19, no. 2. pp. 118–129. Available at: http://nbuv.gov.ua/UJRN/bezin_2013_19_2_8

21. Diorditsa I. V. (2020) Poniattia ta zmist kibershpyhunstva. *Naukovi pratsi Natsionalnoho universytetu "Odeska yurydychna akademiia"*, vol. 26, pp. 49–55. Available at: http://naukovipraci.nuoua.od.ua/arhiv/tom26/9.pdf

22. Dubov D. V. (2014) Kiberprostir yak novyi vymir heopolitychnoho supernytstva: monohrafiia. Kyiv: NISD. 328 p. Available at: https://niss.gov.ua/sites/default/files/2015-02/Dubov_mon-89e8e.pdf

23. Korsun K. (2021) Ohliad rynku kiberbezpeky Ukrainy / Stakeholders' dialogue in the process of Ukraine's integration into the EU Digital Single Market" Project of European Media Platform. Available at: https://eump.org/media/2021/ukraine-into-dsm/korsun_ukr.pdf

24. Kotukh Ye. V. (2021) Kiberbezpeka u publichnomu sektori : monohrafiia. Kharkiv: Kolehium, 272 p.

25. Yakubivska Yu. (2014) Tsilovi ataky v konteksti promyslovoho shpyhunstva. Available at: http://dspace.wunu.edu.ua/jspui/bitstream/316497/1537/1/10_%D1%84%D0%B0%D1%85.pdf

26. Baker K. (2023) What is Cyber Espionage? Available at: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

27. Neumann P. (1995) Computer-Related Risk. ACM Press/Addison Wesley.

28. O'Harat G. (2009) Cyber-espionage: a growing threat to the american economy. *Commlaw conspectus,* vol. 19, pp. 241–275. Available at: https://scholarship.law.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1522&context=commlaw

29. Frankenfield J. (n.d.) Cybrsecurity: Meaning, Types of Cyber Attacks, Common Targets. Available at: https://www.investopedia.com/terms/c/cybersecurity.asp

30. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy», vid 05.10.2017 No. 2163-VIII. *Vidomosti Verkhovnoi Rady (VVR).* 2017. No. 45. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text

31. Cyber espionage. (2020) ENISA Threat Landscape. 10 p. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage/@@download/fullReport

32. From Espionage to Cyber Espionage. (n.d.). Available at: https://www.cyber-espionage.ch/

33. What is Cyber Espionage? (n.d.) Vmware. Available at: http://www.vmware.com/topics/glossary/content/cyber-espionage.html

34. Study on the scale and impact of industrial espionage and theft of trade secrets through cyber. (2019). Pwc. Available at: https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf

35. Bigelow J. Sentonas M. (2014) The economic impact of cybercrime and cyber espionage. Available at: https://www.securitysolutionsmedia.com/2014/03/11/the-economic-impact-of-cybercrime-and-cyber-espionage/

36. EU Cyber Resilience Act: what to watch out for now. (2023). Available at: https://onekey.com/blog/eu-cyber-resilience-act-what-to-watch-out-for-now/

37. Industrial espionage: the threat to global business. (n.d.). Available at: https://www.enderi.fr/Industrial-Espionage-The-Threat-to-Global-Business_a1143.html

38. 6 Ways Cybercrime Impacts Business. (n.d.). Available at: https://www.investopedia.com/financial-edge/0112/3-ways-cybercrime-impacts-business.aspx

39. The impact of cybersecurity threats and cybercrime on businesses. (n.d.). Available at: https://www.bitsioinc.com/cybercrime-impact-on-businesses/