Електронне наукове фахове видання "**Ефективна економіка**" включено до переліку наукових фахових видань України з питань економіки (Наказ Міністерства освіти і науки України від 29.12.2014 № 1528)
www. economy.nayka.com. ua | № 5, 2019 | 30.05.2019 р.

DOI: 10.32702/2307-2105-2019.5.45

УДК 338

Г. Г. Маліцька,
дослідник кафедри економіки підприємства та управління персоналом,
Чернівецький національний університет імені Юрія Федьковича
ORCID: 0000-0002-1064-0656
Н. Я. Кутаренко,
кандидат економічних наук,
асистент кафедри економіки підприємства та управління персоналом,
Чернівецький національний університет імені Юрія Федьковича
ORCID: 0000-0002-3507-8700

ПРОМИСЛОВЕ ШПИГУНСТВО В КОНТЕКСТІ ЕКОНОМІЧНОЇ ЗЛОЧИННОСТІ

H. H. Malitska
researcher of enterprise economics and human resources management department,
Yurii Fedkovych Chernivtsi National University, Chernivtsi
N. Ya. Kutarenko
candidate of Economic Sciences,
assistant of enterprise economics and human resources management department,
Yurii Fedkovych Chernivtsi National University, Chernivtsi

INDUSTRIAL ESPIONAGE IN THE CONTEXT OF ECONOMIC CRIME

У статті досліджується поняття економічної злочинності та промислового шпигунства. Виділено три основні визначення поняття «економічна злочинність»: економічна злочинність як всі види злочинів, що зазіхають на економіку; економічна злочинність як злочини проти власності; економічна злочинність як господарські злочини. Зазначено ознаки економічних злочинів. Досліджено наявність економічної злочинності серед українських організацій та підприємств. Виділено п'ятірку найбільш поширених економічних злочинів та шахрайства протягом останніх двох років, серед яких: незаконне привласнення майна, шахрайство у сфері закупівель, хабарництво та корупція, шахрайство у сфері управління персоналом та кіберзлочини. Розглянуто поняття промислового шпигунства. Наведено порівняльну характеристику промислового шпигунства та конкурентної розвідки шляхом співставлення методів їх здійснення. Виділено основні типи інсайдерських загроз в контексті промислового шпигунства. Розглянуто основні групи методів, які використовуються промисловими шпигунами. А також зазначено основні кроки компанії, які допоможуть вирішити проблему промислового шпигунства.

The article deals with the concept of economic crime and industrial espionage. There are three main definitions of "economic crime": economic crime as all kinds of offenses that encroach on the economy; economic crime as property crimes; economic crime as economic crimes. Signs of economic crimes are mentioned. The existence of economic crime among Ukrainian organizations

and enterprises was investigated. Five of the most widespread economic crimes and fraud over the past two years have been identified, including illegal property appropriation, procurement fraud, bribery and corruption, fraud in the field of human resources management and cybercrime. A comparison has been made of the number of cases of economic crime over the past two years and highlighted the possible causes of their occurrence and development. The concept of industrial espionage is considered. The comparative characteristic of industrial espionage and competitive intelligence by comparison of methods of their implementation is given. The main types of insider threats in the context of industrial espionage are highlighted. The main groups of methods used by industrial spies are considered. Analytical methods of industrial espionage, such as the introduction of their rights and recruitment. The technical methods of industrial espionage are disclosed through the description of the possibility of using various technical means for the implementation of industrial espionage. Another element of industrial espionage, namely insider information, is highlighted. It also highlights the company's key steps to address the issue of industrial espionage. These steps are divided into groups depending on the ability to use the company at different levels of activity. To the micro level is the formation of a system of preventive measures in order to avoid the occurrence of the fact of industrial espionage. At the macro level, effective state regulation, tax regulation, harmonization of legislation, and stimulation of intelligence and counter-intelligence activities are called for the necessary conditions for the formation of a system of protection against industrial espionage.

Ключові слова: *економічна злочинність; промислове шпигунство; конкурентна розвідка; агентурні та технічні методи промислового шпигусництва; інсайдерські загрози.*

Key words: *economic crime; industrial espionage; competitive intelligence; agent and technical methods of industrial espionage; insider threats.*

Постановка проблеми. Швидкий розвиток ринкових відносин та технологій на сьогоднішній день супроводжується стрімким розвитком і економічної злочинності, від негативних наслідків якої потерпають все більше підприємств та організацій. Це стимулює суб'єктів господарювання розробляти не лише стратегічні плани господарської діяльності, а й стратегії захисту усієї інформації, що стосується їх діяльності.

Сьогодні, при здійсненні діяльності та дослідженні конкурентів, деякі компанії обирають не зовсім законні способи та займаються промисловим шпигунством. Промислове шпигунство стало досить поширеним явищем у світі саме завдяки великому різноманіттю способів та методів його здійснення. Такий тип економічних злочинів є чи не найнебезпечнішим для компаній та організацій у всьому світі.

Аналіз останніх досліджень і публікацій. Серед вітчизняних науковців, котрі зосереджують свої дослідження на даному питанні, можемо виділити наступні: В.Ю. Богданович, В.І. Мельник, Ю.Є. Якубівська, В.В. Зянько, О.І. Кравченко, К.В. Юртаєва та ін.

Формулювання цілей статті. Основною метою публікації є дослідження сутності економічної злочинності, а також промислового шпигунства, як виду незаконних та протиправних дій в підприємницькій діяльності, визначення ознак та методів його здійснення.

Виклад основного матеріалу дослідження. В умовах технологічного та інформаційного розвитку національних економік стрімко поширюється на набирає обертів економічна злочинність. Злочини в сфері економіки становлять реальну небезпеку для країни в цілому та окремих її громадян, оскільки від стану та розвитку економіки залежить існування та життєдіяльність суспільства, а також окреслення рекомендацій щодо його уникнення.

Аналіз літературних джерел та нормативно-правових актів дає змогу виділити три основні значення «економічної злочинності». Найбільш розповсюдженим визначенням поняття «злочинності у сфері економіки» є наступне: це усі види злочинів, які зазіхають на економіку, права, свободи, потреби учасників економічних відносин і порушують нормальне функціонування економічного механізму, спричиняють шкоду різним соціальним цінностям і благам. Відповідно до іншого підходу, економічна злочинність – це злочини проти власності, господарські та корисливі службові злочини. Згідно із найвужчим визначенням економічна злочинність – це, перш за все, злочини проти власності та господарські злочини[4, с.359].

Якщо узагальнити різні визначення поняття «економічна злочинність», можна сформулювати наступне: економічна злочинність – це протиправна дія, яка вчиняється у сфері економіки із зловживанням влади, що посягає на порядок здійснення економічного управління та має на меті одержання економічної вигоди [8].

Серед ознак економічних злочинів можна виділити:

- характеризуються зловживанням влади;
- мають майновий характер;
- мають високу латентність;
- характеризуються використанням легальної та нелегальної господарської діяльності.

Найбільш вагомим фактором, який приваблює злочинців до здійснення економічного злочину є розвиток та поширення кризових ситуацій в економіці, а також боротьба за економічну владу, що дає можливість розширювати поле для застосування кримінальних способів заволодіння нею та здійснення протиправних дій у сфері економіки.

Економічна злочинність є значною проблемою для українських компаній та підприємств. Відповідно до проведених досліджень 2018 року, 48% українських організацій постраждали від випадків економічних злочинів та шахрайства протягом останніх двох років, порівняно з 43% у 2016 році [3].

Хабарництво та корупція залишається одним із основних видів економічних злочинів, негативний вплив яких відчувають українські організації – 73% респондентів відповіли, що їхні організації стали жертвами випадків хабарництва та корупції протягом останніх двох років. До п'ятірки найбільш поширених видів економічних злочинів та шахрайства також входять: незаконне привласнення майна, шахрайство у сфері закупівель, шахрайство у сфері управління персоналом та кіберзлочини (Рис. 1)

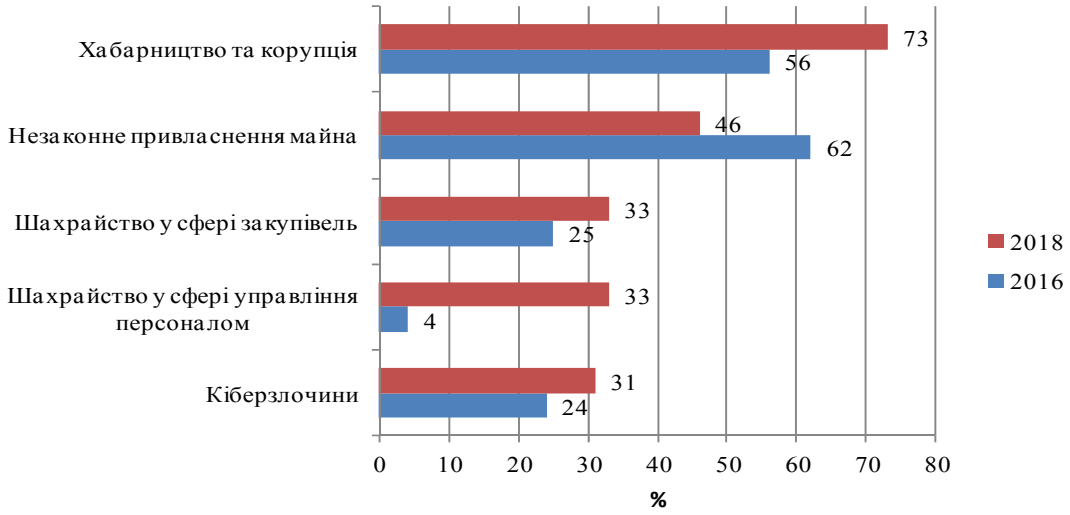

Рис. 1. Топ 5 видів економічних злочинів та/або шахрайства в 2018 році [3]

Рівень хабарництва та корупції в українських організаціях виріз із 56% у 2016 році до 73% у 2018 році. У світі, лише 25% респондентів відповіли, що їхні організації стикалися з випадками хабарництва та корупції, що майже втричі менше порівняно з українськими організаціями. Також, за результатами дослідження, кожний третій український респондент зазначив, що його організація отримувала пропозицію дати хабаря протягом останніх двох років. Викликає занепокоєння той факт, що 23% українських респондентів очікують, що хабарництво та корупція, з поміж інших видів економічних злочинів, буде найбільш суттєвим для їхніх організацій з точки зору фінансових збитків або інших наслідків у наступні два роки.

Показник випадків незаконного привласнення майна зменшився з 62% у 2016 році до 46% у 2018 році. Падіння показника цього виду економічного злочину може бути наслідком посилення контролю в українських організаціях та збільшення інвестицій у засоби для запобігання йому, які вже демонструють свою ефективність.

Результати опитування за 2018 рік показали, що 33% організацій в Україні стикалася з шахрайством у сфері закупівель, що на 11% більше ніж в організаціях світу. Часто випадки шахрайства у сфері закупівель трапляються в організаціях, які неефективно перевіряють постачальників на доброчесність та відсутність у них конфлікту інтересів, та які не мають механізмів контролю за вибором постачальників, укладанням з ними договорів та процесом оплати за їхні товари та послуги.

Шахрайство у сфері управління персоналом розділило третє і четверте місце сере видів шахрайства в українських організаціях, порівняно з восьмим місцем у світових компаніях. Крім того, даний показник стрімко зріс з 4% у 2016 році до 33% у 2018 році. Значно зросла обізнаність про шахрайство у сфері управління персоналом та його сприйняття як справжнього шахрайства. Цей вид шахрайства може значно погіршити професійну етику та поведінку працівників, а також їх лояльність до організації.

Кількість кіберзлочинів, яких зазнають організації, неухильно зростає з року в рік, і цей вид економічного злочину несе високий ризик як для організацій комерційного, так і державного сектору. Результати опитування за 2018 рік свідчать про зростання числа кіберзлочинів проти організацій в Україні на 7% порівняно з 2016 роком. Розвиток технологій призвів до виникнення ряду нових загроз для організацій, серед яких: шкідливе програмне забезпечення, фішинг, сканування мережі та атаки методом підбору паролю. А оскільки 16% українських респондентів переконані у вірогідності того, що їхня організація постраждає від кіберзлочинів у наступні два роки, організаціям та компаніям в Україні слід приділити максимальну увагу цьому виду економічних злочинів.

У багатьох компаніях функції етики та управління ризиками закріплені за окремими підрозділами і зрідка розглядаються як єдине стратегічне ціле. Такий підхід може призвести до того, що ті чи інші сфери діяльності організації залишаються неохопленими, тож випадки економічних злочинів можна легко замовчувати чи вважати проблемою інших підрозділів, попри негативний вплив такого підходу на загальну ефективність заходів із запобігання злочинам, фінансові результати та відносини з регуляторами.

Розробка та впровадження механізму співробітництва та координації різних підрозділів організації, відповідальних за розслідування економічних злочинів, дозволить організації підвищити ефективність оцінки та управління ризиками на горизонтальному рівні, а також врахувати отримані результати в процесі прийняття стратегічних рішень.

Проведені опитування виявили значне збільшення випадків скоєння економічних злочинів в українських компаніях співробітниками (з 28% у 2016 році до 56% у 2018 році), з поміж яких частка економічних злочинів, скоєних вищим керівництвом, також суттєво зросла (з 27% у 2016 році до 55% у 2018 році). Більше того, протягом останніх двох років кількість економічних злочинів, скоєних співробітниками організації, майже в два рази більше, ніж кількість економічних злочинів, скоєних третіми особами.

Однак, однією із найсерйозніших загроз для компаній є не її працівники, а контрагенти. Це треті сторони, з якими організація має постійні прибуткові відносини – агенти, постачальники та клієнти. Це ті фізичні та юридичні особи, від яких компанії очікують певну взаємну довіру, але які, натомість, можуть здійснювати економічні злочини. Зважаючи на результати досліджень, компаніям та організаціям в Україні варто посилити управління ризиками щодо взаємодії з третіми сторонами, як основний захід із запобігання економічним злочинам.

В контексті економічної злочинності варто звернути увагу на поняття промислового шпигунства, яке, в більшості випадків, здійснюється з метою подальшого неправомірного впливу на компанію чи організацію, тобто з метою завдання шкоди.

Сьогодні промислове шпигунство, як цілеспрямований збір інтелектуальних і конфіденційних даних у неетичній та незаконній формі, стрімко процвітає та включає в себе співробітників, що працюють в якості таємних агентів, хакерів, найнятих команд зломщиків, збору, вивчення сміттєвих контейнерів, прослуховування засобів зв’язку тощо [9, с. 159].

Промислове шпигунство являє собою приховану, найчастіше незаконну практику дослідження конкурентів з метою отримання переваги в бізнесі. Ціллю такого роду діяльності може бути незаконне отримання комерційної таємниці, наприклад, специфікації продукту або формули, інформації про бізнес-плани тощо. У багатьох випадках промислові шпигуни просто шукають будь-які дані, котрі їхня організація може використати на свою користь [10, с. 370].

Варто наголосити, що промислове шпигунство відрізняється від конкурентної розвідки. Конкурентні розвідка – це постійний законний процес збору, нагромадження, аналізу даних про внутрішнє і зовнішнє середовище підприємства та надання вищому менеджменту інформації, що дозволяє йому передбачити зміни в зовнішньому середовищі і приймати своєчасні оптимальні рішення щодо управління ризиками [7, с. 132]. Конкурентною розвідкою, як і шпигунством, зазвичай займаються фахівці. Головна відмінність конкурентної розвідки від шпигунства – методи й способи отримання інформації. Все, що використовується розвідником, є законним. Промислове шпигунство, навпаки, передбачає нелегальні методи і технології (Рис. 2).

Рис. 2. Методи проведення конкурентної розвідки та промислового шпигунства [6]

Служба конкурентної розвідки користується тільки відкритими джерелами, основна робота розвідника – інформаційно-аналітична, тобто збирання й опрацювання різних даних, що впливають або можуть негативно чи позитивно вплинути на розвиток бізнесу. Шпигунство полягає, головним чином, в оперативній роботі, зокрема й у вербуванні інсайдерів та збиранні конфіденційної інформації для досягнення конкурентних переваг. Крім того, промислове шпигунство передбачає лише збирання інформації, як правило, досить чітко вказаної замовником. Конкурентна розвідка орієнтована не тільки на збір і аналіз різних даних, а й на вироблення управлінських рекомендацій та рішень, а також на прогнозування можливих дій конкурентів або змін ринку [6, с. 85].

Основна філософія промислового шпигунства полягає в гіпотезі – «навіщо витрачати час та кошти на дослідження, розробку та розвиток, якщо можна підкупити співробітника серед персоналу конкурента» [9, с. 158].

В сучасному світі рівень промислового шпигунства процвітає і включає найрізноманітніші методи: від використання випадкових співробітників, що працюють в якості таємних агентів, хакерів, найманих команд грабіжників до вивчення сміттєвих контейнерів, підслуховування тощо. Промисловий шпигун може являти собою внутрішню загрозу, виступаючи в якості фізичної особи, котра отримала роботу в компанії з метою нелегітимного шпигунства, або незадоволеного співробітника, який торгує інформацією в корисливих цілях або з метою помсти керівництву чи інших корисливих мотивів. Шпигуни можуть також проникнути в довіру співробітників в якості формування соціальної політики підприємства та за допомогою методів психологічного впливу отримувати необхідну конфіденційну інформацію. Для великих підприємств поширеними є випадки, коли промислові шпигуни фізично порушують встановлені керівництвом норми поведінки: переглядаючи корзини для сміття або копіюючи файли чи жорсткі диски комп'ютерів, що залишені без нагляду.

Виділяють чотири типи інсайдерських загроз в контексті промислового шпигунства [10, с. 368]:

1. хабарництво – конкурент або агент розвідки (найнятий конкурентом) звертається до співробітника цільової компанії із пропозицією та стимулюванням до витоку конфіденційних даних, мотивуючи їх готівкою або іншим методом матеріального та нематеріального стимулювання;

2. група змови – виникає у випадку, коли декілька співробітників, групуючись разом, використовують свої колективні знання і привілеї, щоб отримати доступ до конфіденційної інформації компанії;

3. соціальна інженерія – система маніпуляцій мережевими адміністраторами та IT-персоналом, а також інсайдерами або аутсайдерами, які мають доступ до конфіденційної інформації компанії;

4. управлінські привілеї – нелегітимні дії в контексті порушення принципу конфіденційності інформації на підприємстві співробітниками, які використовують свої управлінські повноваження для доступу до службової або конфіденційної інформації та подальшого незаконного її розголошення.

Сукупність методів, притаманних промисловому шпигунству, можна об'єднати в дві групи (Рис. 3) [2]:

1. Агентурні методи.
2. Технічні методи.

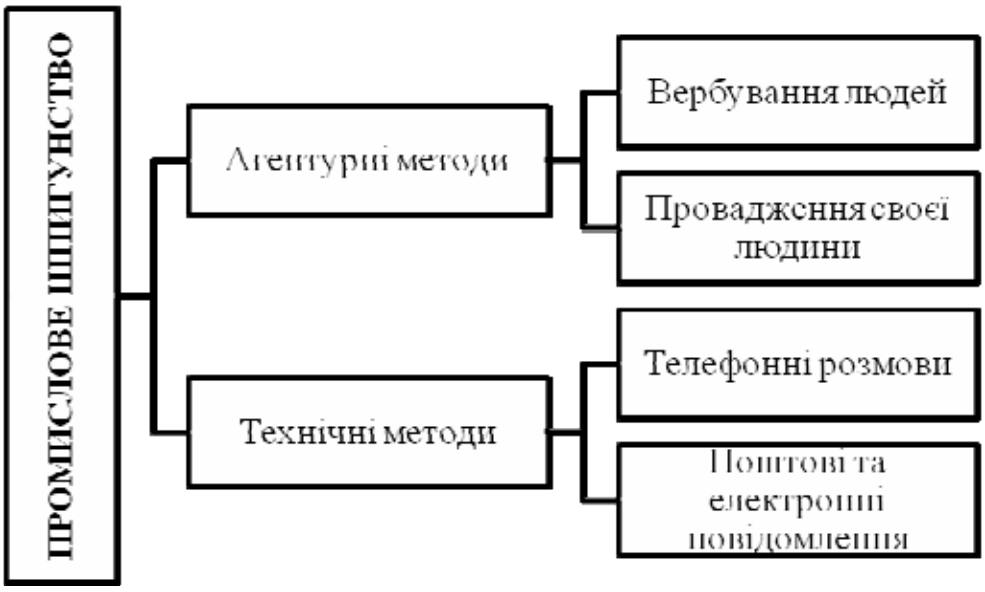

Рис. 3. Методи промислового шпигунства [2]

Агентурний метод отримання інформації – основа будь-якого виду шпигунства. Тут можливі два напрями діяльності: впровадження своєї людини або вербування. У будь-якій комерційній структурі є особи, які за своїми обов'язками й досвідом наближаються до рівня керівництва вищої ланки і які спроможні вести власну гру. Наслідком вербування може бути те, що прибуткові замовлення підуть тим особам, які влаштували бізнес-шпигунство. Якщо кінцевою метою промислового шпигунства є ліквідація фірми-конкурента, або отримання доступу до комерційної таємниці, то впровадження своєї людини має більше переваг в порівнянні з вербуванням, адже рівень довіри до своєї людини є значно вищим. Об'єктами агентурної розробки не завжди є співробітники, які проінформовані щодо справ компанії та планів її розвитку. Будь-який працівник зможе здійснити приховане встановлення спеціальних технічних засобів для отримання інформації з обмеженим доступом [1, с. 18].

Щодо технічних методів промислового шпигунства, то необхідно зауважити, що виробництво і збут спеціальних технічних засобів законодавчо врегульовано, а їх несанкціоноване використання карається законом. Для перехоплення і запису акустичної інформації існує велике різноманіття технічних пристроїв: мікрофони, електронні стетоскопи, радіо-мікрофони, лазерні мікрофони. Непомітне підкидання радіо-передавальних пристроїв – досить поширений спосіб добування інформації. Вони дають змогу протягом декількох годин або декількох днів прослуховувати озвучену в приміщенні інформацію [5, с. 188].

Ще одним елементом промислового шпигунства є інсайдери та їх інформація. Інсайдерами називають людей, які працювали або працюють з конкурентним підприємством чи організацією і володіють конфіденційною інформацією.

Основна проблема захисту інформації підприємства зводиться до необхідності і вміння керівників та робітників зберігати і захищати свою інформаційну власність (інсайдерську інформацію).

На мікрорівні керівництво компанії повинне зосереджувати увагу не лише на реактивних методах забезпечення економічної безпеки, але й формувати систему превентивних заходів з метою уникнення випадків виникнення факту промислового шпигунства [10, с. 370]:

- здійснювати постійний моніторинг потенційних загроз у вигляді шкідливого програмного забезпечення;
- здійснювати періодичну та неперіодичну атестацію персоналу з метою визначення рівня його надійності;
- обов'язково підписувати договори про нерозголошення комерційної таємниці між керівниками підприємств та працівниками, чия професійна діяльність пов'язана з такого роду інформацією.

На макрорівні необхідними умовами формування системи захисту від промислового шпигунства є:

- формування ефективного механізму державного регулювання експорту/імпорту товарів, які містять отриману незаконним шляхом інтелектуальну власність, особливо в якості комерційної таємниці, чи виготовлені на її основі;
- податкове регулювання процесу переміщення через кордон продукції, що виготовлена або реалізується із порушенням права інтелектуальної власності;
- гармонізація законодавства, що стосується захисту від недобросовісної конкуренції у контексті промислового шпигунства, особливо щодо питань, пов'язаних із охороною та захистом комерційної таємниці;

- стимулювання розвідувальної та контррозвідувальної діяльності у контексті боротьби з промисловим шпигунством як на національному, так і на міжнародному рівні, контроль за дотриманням чинного законодавства.

Висновки . Економічна злочинність – це протиправні дії у сфері економіки, пов'язані із зловживанням влади, посяганням на порядок здійснення економічного управління та мають на меті отримання вигоди незаконним шляхом. Вивчення результатів досліджень економічних злочинів дозволяє зробити висновок, що українські підприємства та організації регулярно стикаються із протиправними діями, вчиненими як власними співробітниками, так і третіми особами.

Поруч із економічною злочинністю нами було розглянуто поняття промислового шпигунства. Промислове шпигунство - це один з видів недобросовісної конкуренції, умисне пошкодження промислового обладнання, інформаційних систем на підприємстві, використання психологічного тиску на працівників, що призвело до викрадення комерційною таємниці (нелегальним методом) та можливої подальшої дискредитації або ліквідації бізнесу конкурентів. Варто розділяти поняття промислового шпигунства та конкурентної розвідки, які різняться, в основному, законністю дій. Сьогодні промислове шпигунство здійснюється різними шляхами та методами, що зумовлено розвитком інформаційних технологій та НТП.

З метою убезпечення себе від промислового шпигунства, компаніям необхідно посилювати захист своїх інформаційних ресурсів та проводити постійний моніторинг факторів вразливості інформації, що підлягає захисту.

Список літератури.

1. Богданович В. Ю. Конкурентна розвідка та промислвое шпигунство / В. Ю. Богданович, В. В. Бадрак. // Сучасний захист інформації. – 2014. – №1. – С. 16–22.
2. Виштикалюк М. П. Методи промислового шпигунства в сучасних умовах технологічного розвитку [Текст] / М. П. Виштикалюк // «Перспективи розвитку сучасної науки» (м. Львів, 02-03 грудня 2016 р.). — Херсон : Видавничий дім "Гельветика", 2016. – С. 54-58.
3. Всесвітнє дослідження економічних злочинів та шахрайства 2018 року: результати опитування українських організацій. Виведення шахрайства з тіні [Електронний ресурс] / PWC. — Режим доступу: https://www.pwc.com/ua/uk/survey/2018/economic-crime-survey.html.
4. Дацюк В. Б. Співвідношення економічних злосинів та злочинів у сфері економіки / В. Б. Дацюк// Часопис Київського університету права. – 2011. – №1. – С. 359–363.
5. Зянько В. В. Раціоналізація бізнесової поведінки підприємств України шляхом аналізу переваг та небезпек конкурентної розвідки та промислового шпигунства / В. В. Зянько, В. С. Ревенко // Причорноморські економічні студії. - 2016. - Вип. 6. - С. 187-191.
6. Мельник В. Конкурентна розвідка та промислове шпигунство як засоби конкурентної боротьби / Вікторія Мельник, Ірина Кисельова, Марина Пучкова // Інноваційне підприємництво: стан та перспективи розвитку [Електронний ресурс] : зб. матеріалів II Всеукр. наук.-практ. конф., 29–30 берез. 2017 р. / М-во освіти і науки України, ДВНЗ «Київ. нац. екон. ун-т ім. В. Гетьмана» [та ін.] ; оргком.: Г. О. Швиданенко (голова) [та ін.]. – Електрон. текст. дані. – Київ : КНЕУ, 2017. – С. 84–87. – Назва з титул. екрану.
7. Ожеван М. А. Національна конкурентна розвідка у глобалізованому світі: нові виклики та загрози на тлі «Казусу Сноудена» /М.А. Ожеван // Стратегічні пріоритети. – Київ:НІСД, 2013, № 4 (29). – С.131-139.
8. Скакун Т. О. Економічні злочини: сутнісні ознаки та криміналістичний аналіз їх вчинення [Електронний ресурс]/ – Режим Т.О. Скакун// Ефективна економіка. – 2018. – №3. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=6195.
9. Якубівська Ю. Є. Вплив промислового шпигунства на сферу інтелектуальної власності / Ю. Є. Якубівська // Зовнішня торгівля: право та економіка. Науковий журнал. - № 3(43). 2013. - С.158-162.
10. Якубівська Ю.Є. Цільові атаки в контексті промислового шпигунства / Ю.Є.Якубівська // Проблемы развития внешнеэкономических связей и привлечения иностранных инвестиций: региональный аспект: сб. науч. тр. - Т.2, Донецк: ДонНУ, 2014. – С. 368-372.

References.

1. Bohdanovych, V. Yu. and Badrak, V. V. (2014), "Competitive intelligence and industrial espionage", *Suchasnyi zakhyst informatsii*, vol. 1, pp. 16–22.
2. Vyshtykaliuk, M. P. (2016), "Methods of Industrial Espionage in the Modern Conditions of Technological Development", *Zbirka dopovidej konferentsii* [Conference Proceedings], *Perspektyvy rozvytku suchasnoi nauky* [Prospects for the Development of Modern Science], Lviv, Ukraine 02-03 Dec 2016, pp. 54-58.
3. PwC Ukraine (2018), Worldwide Survey of Economic Crimes and Fraud in 2018: Results of a Survey of Ukrainian Organizations. Outbreak of Shadow Fraud, [Online], available at: https://www.pwc.com/ua/uk/survey/2018/economic-crime-survey.html (Accessed 4 May 2013).
4. Datsiuk, V. B. (2011), "The ratio of economic crimes and crimes in the economy", *Chasopys Kyivskoho universytetu prava*, vol.1, pp. 359–363.

5. Zianko, V. V. and Revenko, V. S. (2016), "Rationalization of Business Behavior of Ukrainian Enterprises by Analyzing the Advantages and Dangers of Competitive Intelligence and Industrial Espionage", *Prychornomorski ekonomichni studii*, vol. 6, pp. 187-191.

6. Melnyk, V. Kyselova, I. and Puchkova, M. (2017), "Competitive intelligence and industrial espionage as a means of competition", *Zb. materialiv II Vseukr. nauk.-prakt. konf., 29–30 berez. 2017* [Collection of materials of the 2nd All-Ukrainian Scientific and Practical Conference, 29-30 March. 2017], *Innovatsiine pidpryiemnytstvo: stan ta perspektyvy rozvytku* [Innovative entrepreneurship: the state and prospects of development], KNEU, Kyiv, Ukraine, pp. 84–87..

7. Ozhevan, M. A. (2013), "National Competitive Exploration in a Globalized World: New Challenges and Threats Against the Background of the "Casu Snowden"", *Stratehichni priorytety*, vol. 4 (29), NISD, Kyiv, Ukraine, pp.131-139.

8. Skakun, T. O. (2018), "Economic crimes intrinsic features and forensic analysis of their commission", Efektyvna ekonomika, vol. 3, [Online], available at: http://www.economy.nayka.com.ua/?op=1&z=6195 (Accessed 4 May 2013).

9. Yakubivska, Yu. Ye. (2013), "Impact of Industrial Espionage on the Sphere of Intellectual Property", *Zovnishnia torhivlia: pravo ta ekonomika. Naukovyi zhurnal*, vol. 3(43), pp.158-162.

10. Yakubivska, Yu.Ye. (2014), "Targeted attacks in the context of industrial espionage", *Problemy razvitija vneshnejekonomicheskih svjazej i privlechenija inostrannyh investicij: regional'nyj aspekt*, vol.2, DonNU, Doneck, Ukraine, pp. 368-372.

Стаття надійшла до редакції 16.05.2019 р.