УДК 005.93:658:336:338 **JEL Classification: D21, M 21, O10**
DOI: https://doi.org/10.32515/2663-1636.2021.7(40).20-30

О.М. Левченко, проф., д-р екон. наук
А.О. Левченко, проф., канд. екон. наук
Т.А. Немченко, канд. екон. наук
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Захист комерційної таємниці в контексті стратегічного управління економічною безпекою організації в умовах цифровізації економіки

У статті розкрито необхідність захисту комерційної таємниці як вагомого етапу формування стратегічного управління економічною безпекою підприємств в мережевій економіці. Визначено сутність категорії комерційної таємниці, її ознаки та особливості. Виокремлено головні загрози комерційній таємниці в умовах становлення цифрової економіки. Проаналізовано основні методи захисту комерційної таємниці та наголошено на особливостях даного процесу під час цифрових трансформацій, зокрема на посиленні інформаційної безпеки та необхідності формування соціально-орієнтованого стратегічного управління кадровими ресурсами

комерційна таємниця, економічна безпека, цифрова економіка, стратегічне управління економічною безпекою, кібербезпека, соціально-орієнтована кадрова стратегія

О.М. Левченко, проф., д-р экон. наук
А.О. Левченко, проф., канд. экон. наук
Т.А. Немченко, канд. экон. наук
Центральноукраинский национальный технический университет, г. Кропивницкий, Украина

Защита коммерческой тайны в контексте стратегического управления экономической безопасностью организации в условиях цифровизации экономики

В статье раскрыта необходимость защиты коммерческой тайны как значимого этапа формирования стратегического управления экономической безопасностью предприятий в сетевой экономике. Определена сущность категории коммерческой тайны, ее признаки и особенности. Выделены главные угрозы коммерческой тайны в условиях становления цифровой экономики. Проанализированы основные методы защиты коммерческой тайны и отмечены особенности этого процесса во время цифровых трансформаций, в частности усиление информационной безопасности и необходимости формирования социально-ориентированного стратегического управления кадровыми ресурсами

коммерческая тайна, экономическая безопасность, цифровая экономика, стратегическое управление экономической безопасностью, кибербезопасность, социально-ориентированная кадровая стратегия

Постановка проблеми. Епоха цифровізації створює передумови для утворення значної кількості загроз щодо стабільного стратегічного розвитку усіх сфер економіки. Цифрові зміни охопили всі сфери функціонування людини: державне управління, бізнес, фінансовий сектор, освіту та сферу послуг, що обумовило переорієнтацію векторів розвитку мережевої економіки у напрямі глобалізації, переходу у віртуальний простір, застосування штучного інтелекту та високих технологій, зростання питомої ваги інтелектуальної праці, зменшення ролі фізичної праці та капіталу. Відповідно, швидкоплинність змін соціально-економічного середовища на сьогодні зумовлює необхідність формування осучасненої системи управління функціонуванням господарських суб'єктів для їх ефективного довгострокового розвитку, характерною ознакою якої буде врахування принципів забезпечення безпеки господарських суб'єктів під час кардинальних стратегічних перетворень та змін.

Маємо зазначити, що одним з головних стрижнів функціонування сучасних підприємств в час цифровізації виступають знання, технології та інформація, цінність не лише надбання, а й збереження яких багато в чому виступає мірилом успішності

суб'єкту господарювання на ринку. Відповідно, питання захисту комерційної таємниці є актуальним, особливо з огляду на перспективу стратегічного розвитку бізнесу, враховуючи швидке зростання обсягу інформації, що відноситься до комерційної таємниці із нарощенням цифровізації та застосування передових технологій в економічній діяльності, загострення конкурентної боротьби на тлі стирання кордонів міжнародних та внутрішніх ринків та, відповідно, використання методів недобросовісної конкуренції, враховуючи відставання темпів відповідності законодавчого захисту цифрових економічних процесів до їх темпів розвитку.

Аналіз останніх досліджень та публікацій. Дослідженням економічних змін в епоху цифровізації здійснювалося багатьма вченими, зокрема, Залужним А., Піжуком О., Батраковою Т., Кузнецовою А. та ін. [2; 9; 17]. Виокремлення основних напрямів змін формуванням системи економічної безпеки за становлення мережевої економіки сформовано Паршиною Ю., Паршиним Ю., Савченком Ю., Передерій Т., Шкарлетом С., Садчиковою І., Нєустроєвим Ю., Єгоровою-Гудковою Т., Острянком В., Сталінською О. та ін. [11; 14; 15; 16; 19; 23]. Підходи до управління комерційною таємницею в бізнесі було здійснено такими науковцями як Белялов Т., Загоруйко В., Лічман Т., Благою В., Шевердіною А., Благим В., Яртим І. та ін. [3; 4; 12; 24]. Однак, на нашу думку, потребують уточнення напрями удосконалення захисту комерційної таємниці як стратегічного об'єкту забезпечення ефективної системи фінансово-економічної безпеки в умовах становлення цифрової економіки.

Постановка завдання. Метою статті виступає дослідження сутності комерційної таємниці в умовах формування цифрової економіки, визначення основних джерел загроз витоку інформації та перспективних напрямів збереження комерційної таємниці для забезпечення ефективного стратегічного управління економічною безпекою господарюючих суб'єктів враховуючи трансформаційні зміни економіки сучасності.

Виклад основного матеріалу. Формуючи систему стратегічного розвитку підприємства варто виходити з необхідності забезпечення його економічної безпеки комплексно, починаючи від організаційної структури, майна та ресурсного забезпечення організації, персоналу та фінансової системи, закінчуючи захистом конфіденційної інформації, яка відіграє одну з ключових ролей для успішної конкурентної боротьби.

Як показують дослідження, саме інформація на сьогоднішній день забезпечує основні конкурентні переваги господарським об'єктам у порівнянні із іншими ресурсами [24]. Однак, варто враховувати цінність її своєчасного використання, що, в свою чергу, зумовлює необхідність її посиленого збереження.

Виходячи із зазначеного, зауважимо, що аналізом питання сутності комерційної таємниці займались багато вчених та практиків, узагальнення наукових пошуків яких відображено у табл. 1.

Як визначено в Цивільному кодексі України, особливостями комерційної таємниці є те, що це, насамперед, секретна інформація, яка у повній чи частковій формі та сукупності її окремих елементів є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить; така інформація має комерційну цінність; була предметом заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію [22].

Загалом, до інформації, що становить комерційну таємницю, як правило, відносять нові технології, технічні рішення, методики виконання робіт та процесів, дані, що отримані внаслідок маркетингових досліджень, інформацію щодо перспективних стратегічних ринкових орієнтирів та напрямів інвестування, дані щодо

виробничого, фінансового та кадрового потенціалу організації, умови укладених на підприємстві угод та контрактів, існуючу систему безпеки, тощо.

Таблиця 1 – Узагальнення поглядів науковців щодо сутності комерційної таємниці

Автор	Визначення
Блага В., Шевердіна А., Благой В. [4]	Комерційна таємниця - інформація конфіденційного характеру, що безпосередньо пов'язана з підприємницькою діяльністю суб'єктів права на цю діяльність та надає перевагу у конкурентній боротьбі через її невизначеність.
Яртим І. [24]	Комерційна таємниця - інформація, яка має цінність для його діяльності, невідома іншим особам та знаходиться в обмеженому доступі на законних підставах, стосовно до якої вжито охоронні заходи та яка не є об'єктом інших таємниць.
Белялов Т., Загоруйко В. [3]	Під комерційною таємницею підприємства слід розуміти відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами й іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) якої може заподіювати збиток його інтересам.
Ткачук І. [20]	Комерційна таємниця – конфіденційність інформації, що дозволяє її власникові при існуючих або можливих обставин збільшити доходи, уникнути невиправданих витрат, зберегти положення на ринку товарів, робіт, послуг або отримати іншу комерційну вигоду; інформація, яка становить комерційну таємницю, – науково-технічна, технологічна, виробнича, фінансово-економічна або інша інформація (в тому числі складова секретів виробництва (ноу-хау), яка має дійсну або потенційну комерційну цінність в силу невідомості її третім особам, до якої немає вільного доступу на законній підставі й у відношенні якої власником такої інформації введений режим комерційної таємниці
Господарський кодекс України [7]	Комерційна таємниця - відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, що не є державною таємницею, розголошення яких може завдати шкоди інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею. Склад і обсяг відомостей, що становлять комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання

Джерело: сформовано авторами за [3; 4; 7; 20; 24]

Опрацювання доробків вчених та положень, викладених у нормативних документах, дозволяє стверджувати, що до комерційної таємниці не відносять установчі документи; дані, які передбачені для оприлюднення у державній звітності; відомості, які необхідні для нарахування та сплати податкових зобов'язань, а також інших обов'язкових платежів; інформацію стосовно чисельності та складу персоналу, їх оплату праці; дані щодо платоспроможності підприємства; дані стосовно

забруднення навколишнього середовища; інформацію, що складає державну таємницю; дані, що є об'єктами авторських та патентних прав, тощо [18].

Враховуючи напрацювання вітчизняних науковців, можемо виокремити специфічні ознаки комерційної таємниці, до яких, насамперед, варто віднести предмет та суб'єкт комерційної таємниці, заборону щодо поширення інформації, яка є комерційною таємницею, нанесення збитку внаслідок її розголошення, а також настання відповідальності та негативних наслідків для осіб, що виступили причиною отримання збитків власникам комерційної таємниці [3].

Стратегічна важливість захисту комерційної таємниці в системі побудови безпечної діяльності підприємства обумовлюється наступними факторами:

- сприяння активізації інноваційної діяльності, що, в свою чергу, стимулюватиме активність підприємництва, формування у компаній додаткових конкурентних переваг;
- формування відносин довіри між державою та бізнесом з умови гарантування реальних процедур захисту конфіденційної інформації та відповідальності за її порушення;
- становлення культури цінності інформації, яка допомагає укріпити моральний, психологічний та етичний клімат в колективі з точки зору розуміння приватності та поваги, що дає можливість знизити ризик потенційних загроз системі безпеки підприємства.

Серед загроз комерційній таємниці прийнято виокремлювати внутрішні та зовнішні загрози. Так, джерела внутрішніх загроз зосереджені всередині організації, а зовнішніх – перебувають поза її межами.

Під внутрішніми загрозами, як правило, розуміють: недоліки в роботі з персоналом підприємства; низький рівень організації роботи з документами, які містять комерційну таємницю підприємства; невирішеність соціальних проблем працівників підприємства; плинність кадрів, відсутність досвідчених фахівців у сфері захисту комерційної таємниці; неефективну роботу служби економічної безпеки; низький технічний рівень захисту від втрати інформаційних ресурсів підприємства [12].

До зовнішніх загроз прийнято відносити промислове шпигунство; незаконні дії конкурентів; протизаконні дії з боку кримінальних структур; неправомірні дії працівників правоохоронних органів, тощо [12].

Маємо зауважити, що серед засобів захоплення комерційної таємниці компаній наймасовішими варто вважати розголошення її персоналом (зумисне та ненавмисне), а також отримання інформації шляхом застосування технологічних атак на систему її захисту. Відповідно саме ці напрямки потрібно розглядати при організації системи економічної безпеки компанії в стратегічній перспективі.

Опираючись на основні тенденції розвитку мережевої економіки, до усталених загроз витоку комерційної таємниці варто додати наступні:

- застаріле обладнання та застосовувані технології, які за рахунок морального зносу та неякісної інтеграції полегшують доступ до конфіденційної інформації за спроби до її несанкціонованого отримання;
- відсутність спеціалістів високої кваліфікації, які здатні забезпечити належну систему захисту інформації під час цілеспрямованих комп'ютерних атак та вірусів;
- відсутність у працівників відповідних вмінь та навичок для виявлення спроб посягання на комерційну таємницю з використанням ІКТ;
- передача електронних даних, що становлять комерційну таємницю стороннім особам за відсутності надання їм статусу «комерційна таємниця»;
- кібершантаж або кібервимагання.

Враховуючи дослідження американських фахівців, втрата 20% конфіденційної інформації, яку класифікують як комерційну таємницю, спричиняє банкрутство компанії протягом місяця у 60 з 100 випадків [24].

Особливо актуальним процес захисту комерційної таємниці стає для стартапів, діяльність яких є інноваційною та перспективною, а також для великих компаній, що займають вагому частку ринку, мають численний штат персоналу, певну репутацію, вартісні проєкти, тощо.

Відповідно, робимо висновок щодо важливості для гарантування економічної безпеки підприємства в стратегічному розрізі надавати такій інформації статус комерційної таємниці для можливості вживання адекватних заходів щодо її захисту в майбутньому.

Аналіз наукової літератури доводить, що загалом виокремлюють дві форми захисту комерційної таємниці: зовнішню та внутрішню, за яких застосовуються заходи організаційного, технічного, психологічного та безпосередньо правового характеру.

Як свідчать напрацювання вчених, першочерговими вважаються саме заходи правового характеру, оскільки їхнім основним завданням є забезпечення ефективного функціонування системи інших заходів щодо захисту комерційної таємниці, серед яких виокремлюють створення положень щодо забезпечення збереження комерційної таємниці, доведення інформації стосовно відповідальності за збереження конфіденційної інформації, а також заключення договорів про матеріальну відповідальність у разі її розголошення [8].

Марущак А.І. до правових форм захисту прав на комерційну таємницю відносить перш за все: звернення до суду з позовом про захист порушених прав; визнання права на комерційну таємницю; відновлення становища, що існувало до порушення права, і припинення дій, що порушують право або створюють загрозу його порушення; визнання недійсними повністю або частково акту державного або іншого органу, що суперечить законодавству і порушує право суб'єкта господарювання на комерційну таємницю; відшкодування збитків, завданих порушенням права суб'єкта господарювання на комерційну таємницю [13].

Чинним законодавством закріплено важливий спосіб захисту об'єктів прав на комерційну таємницю – компенсацію, але вона не тотожна відшкодуванню збитків, і застосовується виключно у випадках, коли суд немає сумніву в наявності у потерпілого збитків, проте визначити їх точний розмір такої компенсації дуже важко, тому що встановлення чітких грошових рамок щодо визначення розміру компенсацій законом є недоцільним [13].

Сутність організаційної форми захисту комерційної таємниці зосереджена на організації самостійних дій, що направлені на її захист. Найпоширенішими методами захисту комерційної таємниці прийнято вважати:

- визначення кола осіб, яким доступні певні види інформації, зокрема шляхом виокремлення режимних зон в організації;
- створення спеціальних підрозділів тапризначення відповідальних осіб, які відповідатимуть за організацію захисту комерційної таємниці;
- розробка системи дозволу доступу до конфіденційної інформації в організації;
- формування системи конфіденціального документообігу в організації, тощо [8; 12; 21].

Технічні заходи захисту комерційної таємниці, передусім, передбачають:

- використання новітніх надійних технічних засобів, що дозволяють налагодити режим охорони інформації;

- використання технічних засобів, що дозволяють виявити потенційні канали витоку конфіденційної інформації;
- проведення регулярного моніторингу системи захисту інформації;
- застосування таких інформаційних носіїв, що унеможливлюють несанкціоноване копіювання конфіденційної інформації;
- застосування надійної системи паролів для доступу до комерційної таємниці, тощо [8; 12; 21].

Психологічні заходи щодо захисту комерційної таємниці направлені насамперед на проведення роз'яснювальної роботи серед персоналу для формування розуміння важливості збереження інформаційної таємниці, налагодження сприятливої атмосфери в колективі, здійснення регулярних перевірок для виявлення потенційного кола осіб, які можуть розголошувати конфіденційну інформацію тощо.

З нарощенням темпів цифровізації більшість конфіденційної інформації зберігається за допомогою використання технічних засобів, а тому популярними способами її захоплення виступають саме кібератаки, які направлені як на дестабілізацію роботи господарського суб'єкта, так і на викрадення даних, які дадуть змогу отримати перевагу у конкурентній боротьбі. Так, зокрема, за свідченнями PwC Ukraine серед усіх видів шахрайства від яких постраждали українські компанії у 2020 році кіберзлочини становили 31%, тоді як у 2016 році їхня питома вага становила 24%. Даний факт приводить до висновку щодо необхідності зростання ролі захисту комерційної таємниці саме за рахунок формування надійної системи кібербезпеки, особливо у галузях які найбільш схильні саме до вказаного вище виду шахрайства [5].

Отже, приходимо до висновку, що розробка програми стратегічного управління економічною безпекою підприємств в мережевій економіці передбачає не лише низку усталених заходів щодо організації та оптимізації діяльності фінансової системи, налагодження економічних та екологічних процесів, управління кадровими ресурсами, а й обов'язкове формування ефективної системи інформаційної безпеки. Насамперед, до обов'язкових напрямів її функціонування варто віднести наступні:

- необхідність постійного оновлення обладнання та технологій, які володіють високим ступенем захисту;
- формування автономних потужностей для зберігання конфіденційної інформації та забезпечення резервних генераторів електричної енергії у разі перебоїв з її постачанням для недопущення зупинки роботи системи захисту;
- формування базису електронної інформації, яка є закріпленою у вигляді комерційної таємниці підприємства.

У той же час, в епоху цифровізації не варто забувати і про налагодження ефективної кадрової політики в компанії, позаяк всі технологічні інновації щодо захисту комерційної таємниці можуть бути даремними за відсутності розуміння та лояльності працівників щодо збереження конфіденційності інформації.

Враховуючи особливості становлення цифрової економіки суспільство постає перед викликами, які потрібно починати вирішувати вже сьогодні. Зокрема, до тенденцій розвитку мережевої економіки варто віднести докорінну зміну ринку праці, що веде за собою переорієнтацію трудової діяльності на цифровий простір, зникнення низки професій, зростання ролі професійного навчання протягом життя, необхідності постійного підвищення кваліфікації, отримання цифрових навичок, знань та вмінь. Така ситуація призведе до того, що частина робочої сили стане неконкурентоспроможною, зросте число безробітних. Спираючись на вищезазначене, зауважимо про ризик втрати значної частини кадрового потенціалу компаніями через їхню не відповідність вимогам ринку, що в свою чергу стане потенційним ризиком

розголошення комерційної таємниці для отримання власної вигоди та нанесення збитків роботодавцям, які вимушені були звільнити некомпетентних працівників. У той ж час зросте конкуренція з боку роботодавців за персонал, який має необхідні знання та навички для успішної конкурентної боротьби на глобалізованих ринках цифрової економіки [10]. Відповідно, з цього випливає ризик розголошення комерційної таємниці внаслідок переманювання цінних працівників, які займали вагомі посади та мали доступ до конфіденційної інформації.

Вищенаведене свідчить, що в стратегічній перспективі забезпечення кадрової безпеки має базуватися на організації якісної системи професійної освіти протягом життя для працівників компанії, які є цінними для її розвитку, а також забезпеченні лояльності кадрового складу шляхом формування сприятливого соціально-психологічного клімату в компанії, корпоративної культури, задоволення потреб персоналу та організації дієвої системи його мотивації.

Загалом організація захисту комерційної таємниці в системі трудових відносин формується за двома напрямами:

- персонал, який має доступ до комерційної таємниці не має права на її розголошення;
- персонал, який не має доступу до комерційної таємниці не повинні займатися збором відповідної інформації для подальшого її неправомірного застосування [21].

Зазначене зумовлює необхідність включення пунктів щодо нерозголошення конфіденційної інформації, яка трактується як комерційна таємниця, до трудових контрактів працівників, яким надається доступ до вказаних даних. Зокрема, доцільним є включення пунктів щодо забезпечення захисту комерційної таємниці до контрактів керівництва компаній із зазначенням інформації про особисту відповідальність за організацію системи захисту комерційної таємниці та обов'язку щодо її нерозголошення. Означені кроки дадуть підставу для юридичної відповідальності у разі настання випадків розголошення комерційної таємниці працівниками чи керівництвом компанії.

Перспективним напрямом для гарантування кадрової безпеки, окрім вищезгаданого, стане, на нашу думку, впровадження соціально-орієнтованої кадрової стратегії, яка, насамперед, дасть змогу:

- сформувати позитивний імідж компанії та підняти цінність для працівників працювати саме з цим роботодавцем, що знизить плинність кадрів, а, відповідно, і ризик витоку конфіденційної інформації;
- наростити якість людського капіталу компанії, що знизить ризик застарівання професіональних компетентностей та формування стабільного колективу організації, який з розумінням ставитиметься до необхідності захисту комерційної таємниці;
- формування системи стимулів та гарантій, які забезпечать лояльність персоналу та знизять ризик переманювання елітних працівників конкурентами.

Загалом, соціально-орієнтована кадрова стратегія являє собою комплекс стратегічних цілей та пріоритетів спрямованих на забезпечення ефективного функціонування кадрової складової діяльності організації, яка дає змогу забезпечити відносний паритет соціально-економічних інтересів роботодавця та його найманих працівників [1].

Основними напрямами впровадження соціально-орієнтованої кадрової стратегії в умовах становлення мережевої економіки виступатимуть:

- наявність соціального пакету з диференціацією за категоріями посад, що включатиме як наявність пільг широкого спектру для загального колективу, так і

індивідуальних пільг для особливо цінних категорій персоналу, націлених на задоволення матеріальних, соціальних, культурних, духовних потреб працівників та їх сімей;

- наявність власної соціальної інфраструктури для задоволення потреб працівників компанії (для потужних організацій);
- організація системи перманентного підвищення кваліфікації та професійного навчання із забезпеченням зростання пільг тим, хто здобув більш високий рівень освіти;
- сприяння налагодженню соціально-психологічного клімату в колективі, атмосфери довіри та взаємопідтримки шляхом застосування усталених та новітніх методик, зокрема гейміфікації;
- розробка механізму участі у прибутках компанії у залежності від трудового внеску, тощо.

Висновки та перспективи подальших досліджень. Узагальнюючи результати проведеного дослідження, варто наголосити, що для ефективної організації економічної безпеки в стратегічній перспективі основоположним завданням вітчизняних підприємств стає формування надійної системи захисту комерційної таємниці як запоруки успішної конкурентної боротьби в умовах цифрової трансформації економіки. Враховуючи бурхливі докорінні зміни, які властиві перехідному етапу становлення цифрової економічної системи, основні напрями системи захисту комерційної таємниці на сьогоднішній день мають бути спрямовані в ключі формування у персоналу відповідальності за збереження комерційної таємниці, а також розвитку технічних можливостей захисту конфіденційної інформації за рахунок нарощення технічного, інноваційного та інтелектуального потенціалів компанії. Перспективні напрями подальших наукових розвідок даної проблематики нами вбачаються у розширенні спектру дослідження процесу управління комерційною таємницею стосовно формування організаційного механізму її захисту в контексті стратегічного забезпечення економічної безпеки компанії.

Список літератури

1. Алавердов А. Р., Алавердова Т. П. Социально ориентированнаякадровая стратегия как допонительноеконкурентное преимущество современной организации. *Современная конкуренция*. 2020. Том 14. №1(77). С. 38-47.
2. Батракова Т. І., Кузнецова А. В. Особливості цифрової економіки в Україні та у світі. *Вісник Запорізького національного університету. Економічні науки*. 2018. № 2. С. 84-89.
3. Белялов Т., Загоруйко В. Організаційно-правове забезпечення захисту комерційної таємниці на підприємстві. *Наука онлайн: Міжнародний електронний науковий журнал.* 2017. №11. URL: https://nauka-online.com/ua/publications/ekonomika/2017/11/organizatsionno-pravovoe-obespechenie-zashhity-kommercheskoj-tajny-na-predpriyatii/(дата звернення: 15.11.2021)
4. Блага В. В., Шевердіна А. В., Благой В. В. Комерційна таємниця: захист, правові аспекти її використання та вплив на економіку підприємств в Україні. *Вісник НТУ «ХПІ»*. 2015. № 60 (1169). С. 141-144.
5. Всесвітнє дослідження економічних злочинів та шахрайства 2020. Результати опитування українських компаній.URL: https://www.pwc.com/ua/uk/survey/2020/gecs-ua-2020-ukr.pdf (дата звернення: 20.11.2021)
6. Ганич І. М. Комерційна таємниця в підприємництві. *Науковий вісник Львівського національного університету ветеринарної медицини та біотехнологій ім. Ґжицького*. 2012. Т. 14, № 1(2). С. 26-30.
7. Господарський кодекс України (зі змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/436-15 (дата звернення: 15.11.2021)
8. Зайцева-Калаур І. Організаційно-правові процедури забезпечення охорони та захисту комерційної таємниці суб'єкта господарювання. *Актуальні проблеми правознавства*. 2018. Вип. 4. С. 110-115.

9. Залужний А. Л. Інформаційно-мережеві виміри сучасної економіки. *Причорноморські економічні студії.* 2020. Вип. 50(1). С. 59-63.
10. Левченко О.М., Немченко Т.А. Соціальний розвиток трудового потенціалу в умовах інноваційних трансформацій: [монографія], Кропивницький: Ексклюзив-Систем, 2021. 272 с.
11. Левченко О.М., Ткачук О.В., Царенко І.О. Соціально-економічні передумови забезпечення національної безпеки в умовах глобалізації. *Економіка і регіон. Науковий вісник Полтавського національного технічного університету імені Юрія Кондратюка*. Полтава, 2018. №1(68). С. 37-46
12. Лічман Т. В. Класифікація та аналіз загроз безпеці комерційної таємниці підприємства. *Вісник Одеського національного університету. Економіка.* 2013. Т. 18, Вип. 1(1). С. 230-233.
13. Марущак А.І. Правові основи захисту інформації з обмеженим доступом: Курс лекцій. Київ: КНТ, 2007. 208 с.
14. Нєустроєв Ю. Г.,Єгорова-Гудкова Т. І., Острянко В. В. Аналіз впливу цифровізації економіки на систему економічної безпеки держави. *Вчені записки університету "КРОК". Серія : Економіка*. 2020. Вип. 4. С. 202-209.
15. Паршина О.А., Паршин Ю.І., Савченко Ю.В. Економічна безпека в умовах діджиталізації: сучасний стан та перспективи розвитку інформаційного суспільства. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2019. № 2. С. 167-174.
16. Передерій Т. С. Стратегія цифрової безпеки підприємства як драйвер цифрової трансформації економіки України. *Вісник економічної науки України*. 2019. № 2. С. 201-204.
17. Піжук О. І. Ключові драйвери цифрової трансформації економіки. *Вісник Київського національного університету технологій та дизайну. Серія : Економічні науки*. 2019. № 3. С. 38–47.
18. Про перелік відомостей, що не становлять комерційної таємниці: Постанова Кабінету Міністрів України від 9 серпня 1993 р. URL: http://zakon4.rada.gov.ua/ laws/show/611-93-п (дата звернення: 12.11.2021)
19. Сталінська О. В. Система економічної безпеки підприємства в умовах розвитку цифрової економіки. *Науковий вісник Міжнародного гуманітарного університету. Серія : Економіка і менеджмент.* 2019. Вип. 38. С. 80-86.
20. Ткачук І. В. Теоретичні основи визначення комерційної таємниці. *Управління фінансово-економічною безпекою.* 2015. № 1. С. 10-14.
21. Тугарова О. К., Шепета О. В. Організаційно-правові питання захисту комерційної таємниці. *Науковий вісник Ужгородського національного університету. Серія : Право.* 2018. Вип. 52(2). С. 85-88.
22. Цивільний кодекс України (зі змінами та доповненнями). URL: http://zakon1.rada.gov.ua/laws/show/435-15 дата звернення: 15.11.2021)
23. Шкарлет С., Садчикова І.Трансформація системи фінансово-економічної безпеки підприємства в умовах цифрової економіки. *Проблеми і перспективи економіки та управління*. 2019. № 3. С. 264-276.
24. Яртим І.А. Комерційна таємниця як фактор забезпечення економічної безпеки реалізації стратегічних змін промислового підприємства. *Глобальні та національні проблеми економіки*. Випуск 3. 2015. С. 510-515.

References

1. Alaverdov, A. R. & Alaverdova, T. P. (2020). Sotsyalno oryentyrovannaia kadrovaia stratehyia kak doponytelnoe konkurentnoe preymushchestvo sovremennoi orhanyzatsyy [Socially-oriented personnel strategy as an additional competitive advantage of modern organization]. *Sovremennaia konkurentsyia - Modern competition, Vol.14, №1(77),* 38-47 [in Russian].
2. Batrakova, T. I. & Kuznetsova, A. V. (2018). Osoblyvosti tsyfrovoi ekonomiky v Ukraini ta u sviti [Features of the digital economy in Ukraine and in the world]. *Visnyk Zaporizkoho natsionalnoho universytetu. Ekonomichni nauky -Bulletin of Zaporizhia National University. Economic sciences, 2,* 84-89 [in Ukrainian].
3. Belialov, T. & Zahoruiko, V. (2017). Orhanizatsiino-pravove zabezpechennia zakhystu komertsiinoi taiemnytsi na pidpryiemstvi [Organizational and legal support for the protection of commercial secrets at an enterprise]. *Nauka onlain: Mizhnarodnyi elektronnyi naukovyi zhurnal - Science online: International electronic scientific journal, №11.* Retrieved from https://nauka-online.com/ua/publications/ekonomika/2017/11/organizatsionno-pravovoe-obespechenie-zashhity-kommercheskoj-tajny-na-predpriyatii/ [in Ukrainian].
4. Blaha, V. V., Sheverdina, A. V. & Blahoi, V. V. (2015). Komertsiina taiemnytsia: zakhyst, pravovi aspekty yii vykorystannia ta vplyv na ekonomiku pidpryiemstv v Ukraini [Trade secret: protection, legal

aspects of its use and impact on the economy of enterprises in Ukraine]. *Visnyk NTU «KhPI» – Bulletin of NTU "KhPI", № 60 (1169),* 141-144 [in Ukrainian].

5. Vsesvitnie doslidzhennia ekonomichnykh zlochyniv ta shakhraistva 2020. Rezultaty opytuvannia ukrainskykh kompanii[World Survey of Economic Crimes and Fraud 2020. Survey results of Ukrainian companies]. Retrieved from https://www.pwc.com/ua/uk/survey/2020/gecs-ua-2020-ukr.pdf [in Ukrainian]
6. Hanych, I. M. (2012). Komertsiina taiemnytsia v pidpryiemnytstvi [Commercial secret in business]. *Naukovyi visnyk Lvivskoho natsionalnoho universytetu veterynarnoi medytsyny ta biotekhnolohii im. Gzhytskoho - Scientific Bulletin of Gzhytskyi Lviv National University of Veterinary Medicine and Biotechnology, Vol. 14, № 1(2),* 26-30 [in Ukrainian].
7. Hospodarskyi kodeks Ukrainy (zi zminamy ta dopovnenniamy)[Economic Code of Ukraine (as amended)]. Retrieved from https://zakon.rada.gov.ua/laws/show/436-15 [in Ukrainian].
8. Zaitseva-Kalaur, I. (2018). Orhanizatsiino-pravovi protsedury zabezpechennia okhorony ta zakhystu komertsiinoi taiemnytsi subiekta hospodariuvannia [Organizational and legal procedures to ensure the protection and safeguarding of trade secrets of business entity]. *Aktualni problemy pravoznavstva – Current issues of jurisprudence, 4,* 110-115 [in Ukrainian].
9. Zaluzhnyi, A. L. (2020). Informatsiino-merezhevi vymiry suchasnoi ekonomiky[Information and network dimensions of modern economy]. *Prychornomorski ekonomichni studii - Black Sea Economic Studies, 50(1),* 59-63 [in Ukrainian].
10. Levchenko, O.M. & Nemchenko, T.A. (2021). Sotsialnyi rozvytok trudovoho potentsialu v umovakh innovatsiinykh transformatsii [Social development of labour potential in the conditions of innovative transformations]. Kropyvnytskyi: Ekskliuzyv-System [in Ukrainian].
11. Levchenko, O.M., Tkachuk, O.V. & Tsarenko, I.O. (2018). Sotsialno-ekonomichni peredumovy zabezpechennia natsionalnoi bezpeky v umovakh hlobalizatsii[Socio-economic prerequisites for national security in the context of globalization]. *Ekonomika i rehion. Naukovyi visnyk Poltavskoho natsionalnoho tekhnichnoho universytetu imeni Yuriia Kondratiuka. Poltava – Economy and region. Scientific Bulletin of Poltava National Technical University named after Yuri Kondratyuk, 1(68),* 37-46 [in Ukrainian].
12. Lichman, T.V. (2013). Klasyfikatsiia ta analiz zahroz bezpetsi komertsiinoi taiemnytsi pidpryiemstva[Classification and analysis of threats to the security of commercial secrets of the enterprise]. *Visnyk Odeskoho natsionalnoho universytetu Ekonomika – Bulletin of Odessa National University. Economic, Vol. 18, 1(1),* 230-233 [in Ukrainian].
13. Marushchak, A.I. (2007). Pravovi osnovy zakhystu informatsii z obmezhenym dostupom [Legal bases of protection of information with limited access] . Kyiv: KNT [in Ukrainian].
14. Nieustroiev, Yu.H., Yehorova-Hudkova, T.I. & Ostrianko, V.V. (2020). Analiz vplyvu tsyfrovizatsii ekonomiky na systemu ekonomichnoi bezpeky derzhavy [Analysis of the impact of digitalization of the economy on the economic security of the state]. *Vcheni zapysky universytetu "KROK". Seriia : Ekonomika – Scientific notes of KROK University. Series: Economics, 4,* 202-209 [in Ukrainian].
15. Parshyna, O.A., Parshyn, Yu.I. & Savchenko, Yu.V. (2019). Ekonomichna bezpeka v umovakh didzhytalizatsii: suchasnyi stan ta perspektyvy rozvytku informatsiinoho suspilstva[Economic security in the context of digitalization: current status and prospects for the development of information society]. *Naukovyi visnyk Dnipropetrovskoho derzhavnoho universytetu vnutrishnikh sprav – Scientific Bulletin of Dnipropetrovsk State University of Internal Affairs, 2,* 167-174[in Ukrainian].
16. Perederii, T.S. (2019). Stratehiia tsyfrovoi bezpeky pidpryiemstva yak draiver tsyfrovoi transformatsii ekonomiky Ukrainy [Digital security strategy of an enterprise as a driver of digital transformation of Ukraine's economy]. *Visnyk ekonomichnoi nauky Ukrainy-Bulletin of Economic Science of Ukraine, 2,* 201-204 [in Ukrainian].
17. Pizhuk, O.I. (2019). Kliuchovi draivery tsyfrovoi transformatsii ekonomiky[Key drivers of digital transformation of the economy]. *Visnyk Kyivskoho natsionalnoho universytetu tekhnolohii ta dyzainu. Seriia : Ekonomichni nauky – Bulletin of Kyiv National University of Technology and Design. Series: Economic Sciences, 3,* 38–47 [in Ukrainian].
18. Pro perelik vidomostei, shcho ne stanovliat komertsiinoi taiemnytsi: Postanova Kabinetu Ministriv Ukrainy vid 9 serpnia 1993 r. [On the list of information that is not a commercial secret: Resolution of the Cabinet of Ministers of Ukraine of August 9, 1993.] (1993). Retrieved from http://zakon4.rada.gov.ua/laws/show/611-93-p [in Ukrainian].
19. Stalinska, O.V. (2019). Systema ekonomichnoi bezpeky pidpryiemstva v umovakh rozvytku tsyfrovoi ekonomiky [The system of economic security of the enterprise in the digital economy]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriia : Ekonomika i menedzhment – Scientific Bulletin of the International Humanities University. Series: Economics and Management, 38,* 80-86[in Ukrainian].

20. Tkachuk, I.V. (2015). Teoretychni osnovy vyznachennia komertsiinoi taiemnytsi [Theoretical foundations of the definition of commercial secrets]. *Upravlinnia finansovo-ekonomichnoiu bezpekoiu - Financial and economic security management, 1,* 10-14[in Ukrainian].
21. Tuharova, O.K. & Shepeta, O.V. (2018). Orhanizatsiino-pravovi pytannia zakhystu komertsiinoi taiemnytsi [Organizational and legal issues of protection of trade secrets]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo – Scientific Bulletin of Uzhhorod National University. Series: Law, 52(2),* 85-88[in Ukrainian].
22. Tsyvilnyi kodeks Ukrainy (zi zminamy ta dopovnenniamy) [Civil Code of Ukraine (as amended)]. Retrieved from http://zakon1.rada.gov.ua/laws/show/435-15 [in Ukrainian].
23. Shkarlet, S. & Sadchykova, I. (2019). Transformatsiia systemy finansovo-ekonomichnoi bezpeky pidpryiemstva v umovakh tsyfrovoi ekonomiky [Transformation of the financial and economic security of an enterprise in the digital economy] . *Problemy i perspektyvy ekonomiky ta upravlinnia – Problems and prospects of economics and management, 3,* 264-276[in Ukrainian].
24. Yartym, I.A. (2015). Komertsiina taiemnytsia yak faktor zabezpechennia ekonomichnoi bezpeky realizatsii stratehichnykh zmin promyslovoho pidpryiemstva [Commercial secret as a factor in ensuring economic security of the implementation of strategic changes in the industrial enterprise]. *Hlobalni ta natsionalni problemy ekonomiky – Global and national economic problems, 3,* 510-515 [in Ukrainian].

Oleksandr Levchenko, Professor, Doctor of Economic Sciences
Anna Levchenko, Professor,PhD in Economics (Candidate of Economic Sciences)
Nemchenko Tetiana, PhD in Economics (Candidate of Economic Sciences), Assistant Lecturer
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

Protection of Commercial Secrets in the Context of Strategic Management of Economic Security of the Organization in the Context of Digitalization of the Economy

The article substantiates the relevance of developing the mechanism for protecting commercial secrets of the organization in the system of strategic management of economic security of the organization, taking into account the transformational changes in the economy.

Using the methods of synthesis and analysis, logical and generalizing methods, the authors determined the essence and basic features of the concept of "commercial secret" in both legal and scientific literature. The most common threats to commercial secrets have been identified and the sources of threats to the leakage of confidential information have been identified, taking into account the digitalization of economic processes. Four areas of protection of commercial secrets of an organization have been identified: legal, organizational, technical and psychological. The importance of providing valuable information in the strategic perspective of commercial secrets for the formation of the basis for its protection in future were highlighted, as well as those responsible for protecting this information with the consolidation of duties and responsibilities in collective and employment agreements were identified.

In the context of formation of an effective system of strategic management of economic security of organizations in the conditions of transformational changes the directions of improvement of protection of a commercial secret are offered. Taking into account a growing share of cyber fraud and transition to the preservation of information mainly on digital media, the urgency of enhanced protection increases. Thus, the formation of information security using advanced technologies and equipment, attracting highly qualified specialists in this field, monitoring to identify potential sources of information leakage and eliminate them. Considering that most common source of disclosure of trade secrets is the staff of the organization, it is proposed to form a long-term loyalty of employees and their understanding of the importance of protecting confidential information, the introduction of socially oriented personnel strategy.

commercial secret, economic security, digital economy, strategic management of economic security, cybersecurity, socially-oriented personnel strategy

Одержано (Received) 19.11.2021 *Прорецензовано (Reviewed) 02.12.2021*
Прийнято до друку (Approved) 20.12.2021