УДК 334.02

DOI: https://doi.org/10.32841/2413-2675/2019-38-12

Сталінська О.В.
д.е.н., професор,
професор кафедри міжнародних економічних відносин,
ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»
Stalinska Olena
Vasyl Stefanyk Precarpathian National University

СИСТЕМА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ

ENTERPRISE ECONOMIC SECURITY SYSTEM IN DIGITAL ECONOMIC DEVELOPMENT

Анотація. В епоху цифрової економіки нові технології змінюють структури галузей та бізнес-моделі компаній. У статті визначено основні види економічних злочинів, які чинять негативний вплив на українські підприємства, узагальнено теоретико-методологічні аспекти системи економічної безпеки підприємства: мета, основні завдання та основні функціональні складові системи економічної безпеки підприємства. Проаналізовано стан найбільш поширених видів економічних злочинів та шахрайства на підприємствах України. Узагальнено фактори розвитку цифрової економіки та наслідки для економічної безпеки підприємств України. У сучасних реаліях цифрові технології охопили усі аспекти діяльності організації, у той самий час вони одночасно є, і засобом її захисту, і загрозою для організацій. Запропоновано заходи щодо удосконалення системи економічної безпеки підприємств в умовах розвитку цифрової економіки.

Ключові слова: економічна безпека, система, кіберзлочини, кібербезпека, функції комплаєнс, хабарництво та корупція, шахрайство, цифрова економіка.

Постановка проблеми. В умовах розвитку цифрової економіки зростає турбулентність ринкової кон'юнктури та питання забезпечення та підтримання належного рівня економічної безпеки підприємства набувають особливого значення. Відсутність ефективної нормативно-правової бази щодо захисту суб'єктів господарювання від корупції, криміналізації владно-управлінських структур, рейдерства, недобросовісної конкуренції та інших дестабілізуючих чинників змушує підприємства висувати на перше місце питання забезпечення своєї економічної безпеки.

За результатами дослідження, яке провели спеціалісти компанії PricewaterhouseCoopers (PwC) Україна у 2018 року, 48% українських організацій постраждали від випадків економічних злочинів та шахрайства протягом останніх двох років, порівняно з 43% у 2016 році [1] Хабарництво та корупція залишається одним із основних видів економічних злочинів, негативний вплив яких зазнають 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 (46%), шахрайство у сфері закупівель (33%), шахрайство у сфері управління персоналом (33%) та кіберзлочини (31%). Результати дослідження ілюструють, що від випадків економічних злочинів та/або шахрайства 31% респондентів понесли фінансові збитки на суму понад 100 000 дол. США, при цьому 12% респондентів зазначили збитки від 1 млн. дол. США до 50 млн. дол. США. Проте, це ще не всі негативні наслідки. Українські організації відзначають, що від економічних злочинів та шахрайства найбільше постраждали їхня репутація/бренд (50%), відносини з бізнес-партнерами (42%) та взаємодія з регуляторами (38%) [1].

Вищенаведені данні свідчать про те, що компанії сьогодні працюють в умовах, за яких трансформація бізнес-процесів та моделей управління підприємством стає питанням не лише підвищення конкурентоспроможності, а й виживання загалом. Тому українські підприємства повинні трансформувати існуючі системи економічної безпеки у відповідності до мінливих умов.

Аналіз останніх досліджень і публікацій. Вагомою теоретико-методичною базою дослідження економічної безпеки агентів є праці таких зарубіжних та вітчизняних вчених, як: Л. Абалкін, Л. Біркен, В. Геєць, О. Ілляшенко, А. Козаченко, О. Коробчинський, О. Кузнєцов, Б. Мізюк, В. Мунтіян, Л. Шемаєва.

Попри вагомий доробок названих вчених, зміна умов господарювання, розвиток цифрових технологій, зростання конкуренції на внутрішньому та глобальному ринках посилюють необхідність удосконалення системи економічної безпеки підприємств.

Метою статті є узагальнення та удосконалення питань щодо системи економічної безпеки підприємств в умовах розвитку цифрової економіки.

Виклад основного матеріалу. Одним із підходів до трактування суті категорії економічна безпека підприємства є відображення її як системи. Лише комплексний та системний підходи до організації економічної безпеки на підприємстві забезпечать найбільш повною мірою його надійний захист.

Під системою економічної безпеки Л. Донець, розуміє «обмежену безліч взаємозалежних елементів, що забезпечують безпеку підприємства і досягнення ним цілей бізнесу. Складовими елементами такої безпеки є об'єкт і суб'єкт безпеки, механізм забезпечення безпеки, а також практичні дії щодо забезпечення безпеки» [2, с. 51]. Такої думки дотримується і В. Ортинський [3, с. 84].

Козаченко А.В. та інші вважають, що сучасна система управління економічною безпекою повинна бути гнучкою, інтегрованою та відкритою, яка охоплює принципи, прийоми і способи, методи і методики, процедури, алгоритми і моделі, за допомогою яких забезпечується гармонізація інтересів підприємства з інтересами взаємодіючих з ним суб'єктів зовнішнього середовища [4, с. 107].

Найбільш повне трактування надає Отенко І.П., який вважає, що система економічної безпеки підприємства – це структурований комплекс стратегічних, тактичних та оперативних заходів, спрямованих на захищеність підприємства від зовнішніх та внутрішніх загроз та на формування унікальних здатностей протистояти їм в майбутньому [5, с. 36].

Головною метою системи управління економічною безпекою підприємства є попередження кризових ситуацій та мінімізація впливу негативних факторів на діяльність підприємства.

До основних завдань системи економічної безпеки підприємства належать:

збір вихідної інформації щодо можливості виникнення загроз;

оцінка та аналіз основних ризиків підприємства;

прогнозування стану захищеності підприємства при уникненні ризиків або при відшкодуванні їх наслідків;

дослідження інтерфейсної складової економічної безпеки підприємства (обґрунтування безпечності вибору партнерів, клієнтів та співробітників);

недопущення проникнення на підприємство структур економічної розвідки конкурентів, організованої злочинності й окремих осіб із протиправними намірами;

протидія проникненню до віртуальної бази даних підприємства в злочинних цілях;

забезпечення захисту конфіденційної інформації та комерційної таємниці;

забезпечення схоронності матеріальних цінностей підприємства;

багатоетапний захист банківських рахунків підприємства;

захист законних прав і інтересів підприємства і його співробітників;

своєчасне виявлення потенційних злочинних намірів щодо підприємства і його співробітників з боку джерел зовнішніх погроз безпеки;

виявлення, попередження й припинення можливої протиправної й іншої негативної діяльності співробітників підприємства, направлених на зниження рівня його економічної безпеки;

захист співробітників підприємства від насильницьких зазіхань;

формування ефективного інформаційно-аналітичного забезпечення системи управління економічною безпекою підприємства;

формування та інтенсивне використання інноваційного забезпечення системи управління економічною безпекою підприємства;

вироблення та прийняття найбільш оптимальних управлінських рішень щодо стратегії й тактики забезпечення економічної безпеки підприємства;

фізична й технічна охорона будинків, споруд, території й транспортних засобів;

відшкодування матеріального й морального збитку, завданого в результаті неправомірних дій підприємства та окремих співробітників;

здійснення постійного контролю за ефективністю функціонування системи економічної безпеки, удосконалення її елементів [5, с. 36–37].

З урахуванням перерахованих завдань, умов конкурентної боротьби, специфіки бізнесу, технологічних особливостей, конкурентної стратегії, стадії життєвого циклу підприємства вибудовується його система економічної безпеки. Система економічної безпеки кожного підприємства абсолютно індивідуальна. Її повнота й дієвість багато в чому залежать від наявної в державі законодавчої бази, матеріально-технічних і фінансових ресурсів, що виділяє керівник підприємства, розуміння кожним зі співробітників важливості забезпечення безпеки бізнесу.

До системи економічної безпеки підприємства входить цілий ряд елементів (функціональних складових), які відображають основні напрямки його економічної безпеки, і які суттєво відрізняються один від одного за своїм змістом.

Узагальнивши напрацювання вітчизняної та зарубіжної наукової думки щодо досліджуваної проблеми, виділимо наступні основні функціональні складові системи економічної безпеки підприємства:

– фінансова безпека;
– інтерфейсна безпека;
– інформаційна безпека;
– комп'ютерна безпека;
– внутрішня безпека;
– ресурсна (енергетична) безпека;
– екологічна безпека;
– техніко-технологічна безпека;
– кадрова безпека;
– виробнича безпека;
– силова безпека.

При такому складі елементів системи економічної безпеки, вона інтегрується в ресурсно-функціональний підхід при проведенні оцінки та аналізу її рівня [5, с. 39].

Як вже було зазначено раніше, згідно дослідження PwC Україна, до п'ятірки найбільш поширених видів економічних злочинів та шахрайства на підприємствах України входять: хабарництво та корупція (78% респондентів); незаконне привласнення майна (46% респондентів), шахрайство у сфері закупівель (33%), шахрайство у сфері управління персоналом (33%) та кіберзлочини (31%) [1].

Міжнародні дослідження свідчать про негативний стан корупції у приватній сфері в Україні та тенденції її розвитку. Так, за результатами дослідження організації Transparency International за підсумками 2018 року Україна в рейтингу «Індекс сприйняття корупції» набрала 32 бали зі 100 можливих, посіла 122-е місце, поруч із Малі, Малаві та Ліберією. Рейтинг спирається на опитування експертів та бізнесу, які проводить низка міжнародних організацій. Менш корумпованими за сприйняттям, ніж Україна, є всі країни ЄС, включно з Болгарією, яка має найгірші показники в Євросоюзі – 42 бали [6].

Для будь-якого підприємства вжиття заходів щодо обмеження ймовірності і впливу корупції, що може виникати в процесі її діяльності, є ключовим елементом ефективної системи управління ризиками. Це також неодмінна умова виходу на західні ринки і встановлення довгострокових партнерських відносин з компаніями з США, Великої Британії, Німеччини та інших країн, які активізували дотримання правил боротьби з корупцією. Сьогодні комплаєнс став ключовим бізнес-імперативом на сучасному світовому ринку [7].

У контексті протидії корупції у приватній сфері важливого значення набуває запровадження антикорупційного комплаєнсу. Антикорупційний комплаєнс – це система заходів щодо управління ризиками недотри-

мання вимог законів України та інших країн, інших нормативних документів, стандартів та етичних норм (кодексів поведінки), що стосуються боротьби з корупцією [7].

Багато українських організацій все ще не займаються профілактикою шахрайства, а лише реагують або захищаються, коли факт шахрайства вже вчинений: лише 40% опитаних організацій в Україні проводили загальну оцінку ризиків шахрайства протягом останніх двох років; близько третини українських організацій повідомили, що проводили оцінку вразливості до кіберзлочинів. Негативна тенденція спостерігається в більш фокусній оцінці ризиків критичних напрямків діяльності організацій: протидії хабарництву та корупції, боротьбі з відмиванням коштів, або застосуванні санкцій та дотриманні вимог експортного контролю. Крім того, лише 27% українських організацій проводили перевірку дотримання законодавства (due diligence) у сфері протидії хабарництву та корупції в процесі придбання / поглинання іншого бізнесу (порівняно з 45% організацій у світі). Кожна п'ята організація (17%) взагалі не проводила оцінку ризиків протягом двох років, тобто не мають функції комплаєнсу [1].

У багатьох організаціях функції комплаєнс, етики та управління ризиками закріплені за окремими підрозділами і рідко розглядаються як єдине стратегічне ціле. Такий підхід може призвести до того, що ті чи інші сфери діяльності організації залишаються неохопленими, тож випадки шахрайства можна дуже легко замовчувати чи вважати проблемою інших підрозділів, попри негативний вплив такого підходу на загальну ефективність заходів із запобігання шахрайству, фінансові результати та відносини з регуляторами. Важливим кроком, який допоможе подолати відсутність скоординованості дій основних підрозділів, до чиїх функцій входить протидія шахрайству, та дозволить організації підвищити ефективність оцінки та управління комплаєнс, етикою та ризиками на горизонтальному рівні, а також врахувати їх принципи в процесі прийняття стратегічних рішень є розробка та впровадження механізму співробітництва та координації різних підрозділів організації, відповідальних за розслідування випадків шахрайства, за управління ризиками шахрайства та за звітування Правлінню або регуляторам.

У 2018 році значно збільшилися випадки шахрайства в українських організаціях, скоєних співробітниками (з 28% у 2016 році до 56% у 2018 році), з поміж яких частка шахрайства скоєного вищим керівництвом також суттєво зросла (з 27% у 2016 році до 55% у 2018 році) [1]. Більше того, протягом останніх двох років шахрайство, скоєне співробітниками організації, майже в два рази більше, ніж шахрайство, скоєне третіми сторонами. Але однією з найсерйозніших загроз протидії шахрайству, часто є не її працівники, а її контрагенти. Це треті сторони, з якими організація має регулярні та прибуткові відносини – агенти, постачальники та клієнти. Іншими словами, це ті фізичні та юридичні особи, від яких організації очікують певну взаємну довіру, але які, натомість, можуть красти в організації. Зважаючи на результати дослідження, організаціям в Україні варто посилити управління ризиками щодо взаємодії з третіми сторонами (корпоративна розвідка, перевірка доброчесності контрагентів), як основний захід із запобігання випадкам шахрайства [1].

У сучасних реаліях цифрові технології охопили усі аспекти діяльності організації, у той самий час вони водночас є, і засобом її захисту і загрозою для організації – використовуються для скоєння економічних злочинів та шахрайства. Через це, можна стверджувати, що існує ефект замкненого кола: рік за роком технології стають дедалі прогресивнішими, що, у свою чергу, створює простір для збільшення випадків шахрайських дій. Тож організаціям не залишається іншого виходу: вони змушені бути готовими реагувати на дедалі складніші типи шахрайських схем. Якщо сучасні технології використовувати оптимально, вони можуть стати цінним інструментом для захисту організації. 49% українських респондентів відповіли, що технології дозволяють їхнім організаціям забезпечувати постійний моніторинг у режимі реального часу, а 51% переконані, що технології надають їхнім організаціям інформацію, яка дозволяє вживати оперативних заходів для протидії економічним

злочинам та / або шахрайству [1]. Хід прогресу зупинити неможливо, тож сьогодні організаціям доступний величезний вибір з поміж інноваційних та надсучасних технологій для захисту від шахрайства.

В епоху цифрової економіки нові технології змінюють структури галузей та бізнес-моделі компаній. Бізнес розцінює інновації не просто як одну із функцій, а як засіб виживання на ринку. Проте інновації не завжди є вкрай необхідними для бізнесу і до їх впровадження необхідно ставитися досить виважено.

Обсяги ділової активності в Інтернеті зростають з кожним днем. Як споживачі, так і організації дедалі сильніше залежать від ІТ. Поширення Інтернету та поява у повсякденному житті новітніх електронних засобів зробили шахрайство більш витонченим та оригінальним. «Індустрія 4.0» («Четверта промислова революція», «Індустріальний Інтернет» або «Фабрика цифрових технологій») спрямована на повномасштабне переведення усіх фізичних активів і процесів на цифрові технології та їх інтеграцію у цифрові екосистеми з партнерами у ланцюжку створення доданої вартості. Це змінило спосіб ведення бізнесу та функціонування організацій. Інноваційні рішення дозволяють машинам спілкуватися та приймати рішення, а технології штучного інтелекту, робототехніки, дронів та 3D-друку трансформують способи виробництва продукції та виконання повсякденних робочих завдань людиною. ІТ рішення вже стали базовим інструментарієм для функціонування організацій, в той самий час як ІТ організації виходять і на інші ринки: роздрібна торгівля, фінансовий сектор, ринок виробництва та збуту автомобілів.

ІТ рішення створюють нові ринки та послуги, замінюючи собою роботу, яку раніше виконувала людина. Змінюються і принципи взаємодії: на ринку B2C (бізнес-споживач) поширюються інтернет-платформи та електронні сервіси, на ринку B2B (бізнес-бізнес) – смарт-контракти, на ринку B2G (бізнес-уряд) – технології електронного урядування. Та разом з тим, розвиток цифрової економіки створює для організацій нові загрози, серед яких: кібератаки, корпоративне шпигунство та багато інших. У цьому контексті інформаційна безпека стає невід'ємним компонентом успішного функціонування організації. Наведемо деякі характеристики та виклики сучасного цифрового шахрайства: • Нові цифрові продукти створюють простір для нових видів атак. Раніше для того, щоб вивести продукцію на ринок, організації діяли за схемою B2B, тобто: співпрацювали з торговельними посередниками, дистриб'юторами та роздрібними мережами. Сьогодні ж організації активно використовують цифрові платформи B2C, які поєднують їх безпосередньо із споживачами та створюють можливість для істотно різноманітніших видів атак, а отже, і шахрайства. Цифрове шахрайство стає дедалі складнішим, продуманим та руйнівним. За останні роки кібератаки стали доволі поширеним явищем. Сьогодні організації та державні органи у всьому світі потерпають від нового гравця – кібератак, профінансованих державами, здійснених хакерами з політичних чи ідеологічних мотивів, та, вчинених терористичними організаціями. Для цих зловмисників кібератака – це засіб не збагачення, а досягнення тих чи інших геополітичних цілей: порушення діяльності держав, викрадення персональних даних та інтелектуальної власності, збір інформації про структуру інформаційних систем та програмного забезпечення, отримання даних для віддаленого доступу до критично важливої інфраструктури.

За даними дослідження кіберзлочини один із найпоширеніших видів економічних злочинів: від них постраждали 31% організацій в Україні [1]. У світі 49% опитаних керівників стверджують, що можливість стати жертвою кібератаки – це питання часу, а не вірогідності. В Україні 39% керівників також виділяють ризик порушення кібербезпеки як пріоритетний [8].

Кібератаки вражають все на своєму шляху: неважливо, чи це приватна компанія, чи державна установа, чи розташована вона в Україні, чи в іншій частині світу. Організації в Україні з побоюванням ставляться до кіберзлочинів: 16% українських респондентів не лише очікують кібератаки на їхні організації у наступні два роки, а й переконані, що кібератаки будуть найбільш значними для їхніх організацій з точки зору

фінансових збитків або інших наслідків. Та попри це, більшість організацій в Україні не лише недостатньо підготовлені до кібератак, а й не розуміють до кінця ризики, на які наражаються. Так, лише кожна третя організація в Україні (31%) має повністю функціонуючу програму кібербезпеки для захисту від кібератак [1]. Така програма має включати наявні та потенційні ризики для організації, а також перевірений план заходів з реагування на інциденти кібербезпеки. Стандартна практика для організацій, що постраждали від кіберзлочинів, це повідомити державні чи правоохоронні органи про інциденти кібератак. Проте, 28% організацій в Україні відповіли, що вони малоймовірно або й навряд чи будуть повідомляти про такі факти державним або правоохоронним органам (порівняно з 12% респондентів у світі). Більше половини (54%) цих респондентів стверджують, що не впевнені у тому, що у правоохоронних органів є необхідна кваліфікація у цій сфері, а інші 41% – не довіряють правоохоронним органам. Більше третини українських організацій, що зазнали кібератак, постраждали від наслідків шкідливого програмного забезпечення. Внаслідок кібератак були порушені не тільки бізнес-процеси організацій (на думку 51% українських респондентів), а й завдані істотні збитки організаціям[1]. Тому створення сильної кіберстратегії є критично важливим завданням в умовах розвитку цифрової економіки.

Технології, без жодних сумнівів, мають критичне значення у боротьбі з шахрайством, але лише як компонент комплексного рішення. Це тому, що шахрайство є результатом складного поєднання умов та мотивації людей. І організаціям слід приділяти більшу увагу та зосередити зусилля, спрямовані на боротьбу з шахрайством, для мінімізації саме можливостей для скоєння шахрайських дій. Перш за все, слід зосередити зусилля на середовищі, яке впливає на їхню поведінку, а саме: корпоративній культурі на підприємстві. Проведення опитувань, створення фокус-груп та поглиблені інтерв'ю із працівниками можуть використовуватись як засоби для оцінки сильних та слабких сторін корпоративної культури всієї організації. Безперервне навчання та розвиток компетенцій є, також, дуже важливими. Коли працівники чітко розуміють, що саме є неприйнятним і чому, – їм буде значно складніше виправдати для себе шахрайські дії.

Висновки. На сучасному етапі розвитку економіки України значної уваги здобуває питання забезпечення та підтримання належного рівня економічної безпеки підприємства Виявлення та попередження економічних злочинів чи шахрайства – це, поза всіляким сумнівом, комплексне та складне для організації завдання, яке передбачає пошук збалансованого комплексу заходів, які включають технології та людські ресурси, і побудовані на чіткому розумінні стимулів до шахрайських дій та обставин за яких ці дії вчинені. Організаціям вкрай важливо відійти від переконання, що технології є єдиним рішенням або що, до певних меж, шахрайство можна вважати просто частиною операційних витрат організації. Натомість, лише створення корпоративної культури чесності та відкритості в організації за принципом «згори вниз», дозволить побудувати та просувати прозору підзвітність – а це, в свою чергу, дозволить вивести шахрайство з тіні.

З огляду на це стають зрозумілими масштаби необхідної трансформації системи економічної безпеки підприємств, наскільки радикальними повинні бути зміни і чи варто ставитися до них як до інвестицій, що забезпечать повернення вкладених коштів.

Література:

1. Всесвітнє дослідження економічних злочинів та шахрайства 2018 року: результати опитування українських організацій. Виведення шахрайства з тіні. URL: https://www.pwc.com/ua/uk/survey/2018/economic-crime-survey.html (дата звернення: 25.10.2019).
2. Донець Л. І., Ващенко Н. В. Економічна безпека підприємства: навчальний посібник. Київ: Центр навчальної літератури, 2008. 240 с.
3. Ортинський В. Л., Ващенко І. С., Живко З. Б. Економічна безпека підприємств, організацій та установ. Київ: Правова єдність, 2009. 54 с.
4. Козаченко Г. В., Пономарьов В. П., Ляшенко О. М. Економічна безпека підприємства: сутність та механізм забезпечення: монографія. Київ: Лібра, 2003. 280 с.
5. Отенко І. П., Іващенко Г. А., Воронков Д. К. Економічна безпека підприємства: навчальний посібник. Харків: ХНЕУ, 2012. 262 с.
6. Дослідження Transparency International "Індекс сприйняття корупції - 2018. URL: https://ti-ukraine.org/research/indeks-spryjnyattya-koruptsiyi-2018/

7. Окунєв О, Бойко О., Лукін С. Антикорупційний комплаєнс. Посібник для програми з підготовки осіб, відповідальних за реалізацію антикорупційної програми. URL: https://cgpa.com.ua/wp-content/uploads/2018/07/Compliance.pdf (дата звернення: 25.10.2019).
8. Глобальне дослідження KPMG "Виклики, що зростають. Global 2018 CEO Outlook". URL: https://home.kpmg/content/dam/kpmg/ua/pdf/2018/07/CEO-Outlook-2018-ua-v2.pdf

References:

1. Vsesvitnje doslidzhennja ekonomichnykh zlochyniv ta shakhrajstva 2018 roku: rezuljtaty opytuvannja ukrajinsjkykh orghanizacij. Vyvedennja shakhrajstva z tini. Available at: https://www.pwc.com/ua/uk/survey/2018/economic-crime-survey.html (accessed 25 October 2019).
2. Donecj L. I., Vashhenko N. V. (2008) Ekonomichna bezpeka pidpryjemstva [Economic security of the enterprise]. Kyiv: Centr navchaljnoji literatury.
3. Ortynsjkyj V. L., Vashhenko I. S., Zhyvko Z. B. (2009) Ekonomichna bezpeka pidpryjemstv, orghanizacij ta ustanov[Economic security of enterprises, organizations and institutions]. Kyiv: Pravova jednistj.
4. Kozachenko Gh. V., Ponomarjov V. P., Ljashenko O. M. (2003) Ekonomichna bezpeka pidpryjemstva: sutnistj ta mekhanizm zabezpechennja [Economic security of the enterprise: essence and mechanism of providing]. Kyiv: Libra.
5. Otenko I. P., Ivashhenko Gh. A., Voronkov D. K. (2012) Ekonomichna bezpeka pidpryjemstva [Economic security of the enterprise]. Kharkiv: KhNEU. (in Ukrainian)
6. Doslidzhennja Transparency International "Indeks spryjnjattja korupciji - 2018. Available at: https://ti-ukraine.org/research/indeks-spryjnyattya-koruptsiyi-2018 (accessed 25 October 2019).
7. Okunjev O., Bojko O., Lukin S. (2018) Antykorupcijnyj komplajens. Posibnyk dlja proghramy z pidghotovky osib, vidpovidaljnykh za realizaciju antykorupcijnoji proghramy. Available at: https://cgpa.com.ua/wp-content/uploads/2018/07/Compliance.pdf (accessed 25 October 2019).
8. Ghlobaljne doslidzhennja KPMG "Vyklyky, shho zrostajutj. Global 2018 CEO Outlook". Available at: https://home.kpmg/content/dam/kpmg/ua/pdf/2018/07/CEO-Outlook-2018-ua-v2.pdf (accessed 25 October 2019).

Аннотация. В эпоху цифровой экономики новые технологии меняют структуру отраслей и бизнес-модели компаний. В статье определены основные виды экономических преступлений, которые оказывают негативное влияние на украинские предприятия, обобщены теоретико-методологические аспекты системы экономической безопасности предприятия: цель, основные задачи и основные функциональные составляющие системы экономической безопасности предприятия. Проанализировано состояние наиболее распространенных видов экономических преступлений и мошенничества на предприятиях Украины. Обобщены факторы развития цифровой экономики и последствия для экономической безопасности предприятий Украины. В современных реалиях цифровые технологии охватили все аспекты деятельности организации, в то же время они одновременно являются и средством ее защиты, и угрозой для организаций. Предложены мероприятия по совершенствованию системы экономической безопасности предприятий в условиях развития цифровой экономики.

Ключевые слова: экономическая безопасность, система, киберпреступления, кибербезопасность, функции комплаенс, взяточничество и коррупция, мошенничество, цифровая экономика.

Summary. In the digital economy, new technologies are changing the structure of industries and business models of companies. In Ukraine in 2018, 48% of Ukrainian organizations have suffered from economic crime and fraud in the last two years. Companies today operate in a context where the transformation of business processes and enterprise management models becomes not only a matter of increasing competitiveness, but of survival in general. Therefore, Ukrainian enterprises must transform existing economic security systems in the light of changing conditions. The theoretical and methodological aspects of the enterprise economic security system are summarized: the purpose, the main tasks and the main functional components of the enterprise economic security system. The state of the most common types of economic crimes and fraud at the enterprises of Ukraine is analyzed. Factors of digital economy development and consequences for economic security of Ukrainian enterprises are summarized. The article identifies the main types of economic crimes that have a negative impact on Ukrainian businesses: bribery and corruption; misappropriation of property, procurement fraud, personnel management fraud and cybercrime. In the context of combating corruption in the private sphere, the introduction of anti-corruption compliance has been proposed. In today's realities, digital technologies have embraced all aspects of an organization's activities, while being both a means of protecting it and a threat to organizations. It is proposed to create cyber strategies of Ukrainian enterprises, which is a critical task in the conditions of digital economy development. Technologies are without a doubt critical in the fight against fraud, but only as a component of a comprehensive solution. This is because fraud is the result of a complex combination of conditions and people's motivation. The article proposes to focus on the development of corporate culture at the enterprise. The scope of the necessary transformation of the system of economic security of the enterprises becomes clear from the articles, how radical the changes should be and whether they should be treated as investments that will ensure the return of the invested funds. Finding new solutions to improve the economic security of businesses in a digital economy requires the joint efforts of governments, civil society, academia, the scientific community and the technology sector.

Keywords: economic security, system, cybercrime, cybersecurity, compliance functions, bribery and corruption, fraud, digital economy.