5.3. Застосування концепції cyber situational awareness в управлінні економічною безпекою підприємства

Масштабні трансформаційні процеси в економіці України, які супроводжуються глибокими структурними зрушеннями і є важливим фактором динамічного і стабільного розвитку, потребують пошуку та впровадження нових теоретичних і практичних підходів до забезпечення результативного управління економічною безпекою сільськогосподарських підприємств, шляхом створення динамічної системи інформаційно-аналітичного забезпечення всієї сукупності складових внутрішнього потенціалу та ідентифікації зовнішніх тенденцій. Особливої гостроти ця проблема набуває в епоху інформатизації (автоматизації) управлінських процесів.

У сучасних умовах господарювання особливо гостро стоїть питання обґрунтування захисту економічних інтересів українських підприємств, а також прийнятих стратегічних рішень. Євроінтеграційні процеси висувають низку вимог до підприємств України, які змушені адаптуватися до зростання рівня конкуренції та шукати адекватні рішення найскладніших проблем і шляхів зниження загроз своєї діяльності, зумовлені невизначеністю та ризиками. На жаль, сучасні наукові економічні дослідження діяльності національних підприємств, а особливо агропромислового комплексу, не дають цілісного уявлення про безпеку діяльності бізнесу. Зокрема, практично відсутнє уявлення про характер функціонування системи в агресивному середовищі та забезпечення економічної безпеки підприємства в умовах євроінтеграції та глобалізації бізнесу загалом. У нинішніх умовах господарювання постає проблема забезпечення економічної безпеки підприємств, оскільки від її вирішення залежить економічне зростання національної економіки.

Дослідженням питань системи економічної безпеки держави присвячені праці таких вчених, як П. Друкер, К. Мак-Коннелл, П. Самуельсон, А. Сміт, Й. Шумпетер та ін. Система економічної безпеки досліджується в працях таких вітчизняних науковців, як В. Андрійчук, О. Барановський, А. Гальчинський, Т. Клєбанова, О. Малиновська, В. Марнасова, А. Мокій, В. Мунтіян, Г. Пастернак-Таранушенко, В. Шлемко та ін.

Однак, незважаючи на значний внесок науковців та практиків у теорію економічної безпеки підприємства та враховуючи сучасні реалії економічних відносин, залишається низка невирішених раніше питань та проблем, обумовлених сьогоденням.

Ґрунтуючись на теорії Н. Вінера, який доводив, що концептуальні схеми, які визначають поведінку біологічних систем, ідентичні до схем, які реалізуються у складних технічних системах, а отже, їх можна використовувати в соціальному та економічному управлінні, аналізувати на основі тих самих загальних положень теорії управління системами, які створені людьми [1]. Основна ідея, закладена Н. Віннером, полягає в тому, що всесвіт складається із систем, які взаємодіють між собою на основі зворотного зв’язку. Життєздатність системи зумовлюється, здатністю системи сприймати інформацію й адекватно реагувати на отриману інформацію. Йдеться про поняття стійкості системи, а отже, про здатність системи повертатися в рівноважний стан після припинення дії внутрішніх і зовнішніх збурень.

Сучасний підхід до розуміння економічної стійкості є досить одностороннім, оскільки він обмежується рамками фінансових категорій. Під поняттям «стійкість» в економічній літературі більшість науковців та практиків розуміють здатність системи досягати своєї мети, враховуючи зміну внутрішніх та зовнішніх факторів, що призводить, як прав здебільшого до удосконалення її структурного та функціонального змісту.

Одним із важливих питань будь-якої теорії є термінологія та формулювання визначень і категорій. Визначення понять, категорій та дефініцій, що покладені в основу міркувань, логічних побудов, безпосередньо впливають на їх кінцевий результат. Досліджуючи те чи інше явище або процес, важливим є формування категорійного апарату, який ґрунтується на певній методології та системі поглядів, адже саме на цій фазі закладаються основи теорії.

У словнику української мови безпека визначається як «стан, коли кому-, чому-небудь ніщо не загрожує» [2, с. 137].

Г. Л. Вербицька визначає безпеку як заходи або дії, що забезпечують недопущення і оперативне реагування на відповідні загрози заради безпечного функціонування [3].

Ю. М. Великий трактує безпеку як здатність об'єкта, явища, процесу зберігати свою сутність і основну характеристику в умовах цілеспрямованого, руйнівного впливу зовні або в самому об'єкті, явищі, процесі; захист від небезпек на системному рівні; захищеність життєво важливих інтересів об'єкта від загроз (як внутрішніх, так і зовнішніх) [4].

Також зустрічаються визначення безпеки як стану складної системи, коли дія зовнішніх і внутрішніх факторів не призводить до погіршення системи або до неможливості її функціонування і розвитку. Безпека – стан захищеності життєво важливих інтересів особистості, суспільства, організації, підприємства від потенційно і реально існуючих загроз, або відсутність таких загроз.

Проблеми економічної безпеки підприємства порушено в численних працях вітчизняних і закордонних практиків та теоретиків. Аналіз літературних джерел дає змогу стверджувати, що є багато поглядів на визначення поняття «економічна безпека підприємства» (табл. 5.4).

Таблиця 5.4

Визначення економічної безпеки підприємства науковцями та практиками

Автор	Визначення поняття
Капустін Н. [5, с. 12]	сукупність чинників, які забезпечують незалежність, стійкість, здатність до прогресу в умовах дестабілізаційних факторів
Судоплатов А. [6, с. 3]	стан правових, економічних і виробничих відносин, а також матеріальних, інтелектуальних і інформаційних ресурсів, який виражає здатність підприємства до стабільного функціонування
Бєндіков М. [7, с. 8]	захищеність науково-технічного, технологічного, виробничого та кадрового потенціалу підприємства від прямих або непрямих загроз
Сумець О. [8, с. 15]	стан захищеності життєво важливих інтересів підприємства від реальних і потенційних джерел небезпеки чи економічних загроз
Іхваненков С. [9, с. 45]	сукупність умов та чинників, які забезпечують незалежність підприємства, його стабільність і стійкість, здатність до постійного оновлення та самовдосконалення
Ковальов Д. [10, с. 49]	захищеність діяльності підприємства від негативних впливів зовнішнього середовища, а також здатність швидко усунути різні загрози або пристосуватися до наявних умов, що не позначаються негативно на його діяльності
Покропивний С. [11]	стан корпоративних ресурсів (ресурсів капіталу, персоналу, інформації і технології, техніки та устаткування) і підприємницьких можливостей

Аналізуючи визначення поняття економічної безпеки підприємства, можна зазначити наступне:

- застосування понять «система» та «стан системи»;
- використання поняття загрози;
- визначення безпеки, базується на економічних поняттях досягнення мети, функціонування підприємства;
- одночасне використання поняття загрози та економічних показників функціонування підприємства.

Отже, можна визначити спільне:

- існує система (підприємство), яка спрямована на досягнення певної мети (життєво важливих інтересів), має відповідну структуру, взаємозв'язки, перебуває в певному стані, який визначений відповідними параметрами;
- наявність загроз цим параметрам, які мають імовірнісний характер (ризики);
- система характеризується цілісністю – здатністю досягати своєї мети під впливом внутрішніх і зовнішніх факторів та умов зовнішнього середовища.

Метою забезпечення економічної безпеки підприємства має стати система протидії потенційним і реальним загрозам, розробка превентивних заходів щодо усунення чи мінімізація яких має забезпечувати суб'єкту господарювання успішність функціонування в нестабільних умовах зовнішнього та внутрішнього середовища.

При цьому безпека підприємства повинна забезпечуватися за такими основними напрямами: економічна, науково-технічна, інформаційна, кадрова, соціальна, екологічна, фізична тощо.

Прорив інформаційних технологій наприкінці XX початку – XXI сторіччя викликав у світі значні системні перетворення, що дали можливість сформуватись і розвинутись принципово новим й невід'ємним глобальним субстанціям – інформаційному простору та інформаційному суспільству, які мають нині практично необмежений потенціал і відіграють суттєву роль в економічному та соціальному розвитку будь-якої країни світу.

Неконтрольоване поширення та необмежене застосування провідними країнами світу інформаційного простору, як арени дій у процесі сучасного інформаційного протиборства, у свою чергу, поступово призвело до уразливості інформаційної сфери цих країн від впливу внутрішніх і зовнішніх кібернетичних втручань та загроз навмисного, випадкового, природного або штучного характеру тощо [12].

При цьому дедалі очевиднішою стає залежність загального рівня економічної безпеки держави і підприємства від її інформаційної складової.

Можливості, які компанії отримують завдяки впровадженню нових інформаційних технологій, колосальні й охоплюють широкий діапазон. Автоматизовані інформаційні системи здатні забезпечити тісніший взаємозв'язок структурних підрозділів компанії і пристроїв, а ефективне використання даних і аналітики забезпечать більш високу продуктивність і більш індивідуалізовані клієнтські пропозиції. При цьому, вважається, що безпека підвищиться завдяки мінімізації людського фактора, який на сьогодні вважається однією з основних причин збитків у багатьох галузях, шляхом автоматизації завдань, а постійний моніторинг стану та використання аналітики великих масивів даних можуть значно підвищити якість ризик-менеджменту, забезпечуючи високий рівень зменшення і запобігання ризикам, адекватне планування методів і заходів і їх реалізацію у разі реалізації ризиків.

Але ідеалізувати використання автоматизованих інформаційних систем є дуже небезпечним. Як приклад, слід навести діяльність авіакомпаній США:

- липень 2016, комп'ютерний збій в Southwest Airlines [1] призводить до скасування та затримки рейсів на чотири дні, у результаті відмінено близько 800 рейсів. Як пояснила адміністрація компанії: «причиною слугувала технічна несправність у нашій мережі, яка сталася на кількох системах і платформах»;

- серпень 2016 року збій у комп'ютерній системі компанії Delta Airlines [2], компанії довелося скасувати 451 рейс приблизно з 6000, у процесі ліквідації виходу з ладу комп'ютерної системи було скасовано ще 2300 рейсів з 8000.

Важко уявити, до яких збитків призвели ці інциденти.

Все вищеперелічене вимагає переходу до нових методів інформаційно-аналітичного забезпечення управління економічною безпекою підприємств, використання автоматизованих систем управління та сучасних інформаційних технологій.

В останні роки розуміння впливу інформаційного забезпечення на прийняття управлінських рішень, виводить інформацію на новий рівень – як ресурс, що володіє певною цінністю. Інформація стає найважливішим стратегічним ресурсом будь-якого підприємства, її формування та споживання, стає важливою основою ефективного функціонування і розвитку різних сфер суспільної та економічної діяльності [13].

У висновках сьомого щорічного дослідження корпоративних ризиків «Барометр ризиків Allianz 2018» [3] (у межах якого було опитано понад 1911 ризик-менеджерів і страхових експертів з 80 країн), зазначено, що головним ризиком для підприємств на глобальному рівні шостий рік поспіль залишається перерви у виробництві й ланцюзі поставок. Однак більшість компаній стурбовані, що втрати понесені в результаті переривів у виробництві, які зазвичай наступають унаслідок шкоди майну, в майбутньому будуть усе частіше обумовлюватися кібератаками, технічними збоями та геополітичною нестабільністю.

Стурбованість бізнесу викликає й інша глобальна сфера – це інциденти в кіберпросторі, що включають кіберзлочини або злом баз даних, а також технічні збоїв IT-системах.

Ще шість років тому в першому дослідженні «Барометр ризиків Allianz» тільки 1 % респондентів розглядав кіберінциденти як ризик, у 2018 цей ризик посідає другу позицію в рейтингу (табл. 5.5, 5.6).

Загрози можуть змінюватися, але результат залишається тим самим. Перерви у виробництві (включаючи розрив ланцюга поставок) є найбільш значущим ризиком для компаній уже шостий рік поспіль, згідно з даними Барометра ризиків Allianz. Цей ризик вказано в числі трьох найбільш важливих ризиків, що стоять перед компаніями в 2018 році, у 42 % відповідей, на другому місці – кіберінциденти (40 %), на третьому – природні катастрофи (30 %).

---

[1] Final Update and Apology on Systemwide Outages. URL: https://www.southwestaircommunity.com/t5/Southwest-Stories/Final-Update-and-Apology-on-Systemwide-Outages/ba-p/46203.

[2] Delta computers crash, causing delays and cancellations. Experts say it shouldn't have happened. URL: https://www.washingtonpost.com/local/trafficandcommuting/delta-airlines-computer-systems-crash-causing-flight-delays-and-cancellations/2016/08/08/7d5e8fa0-5d72-11e6-af8e-54aa2e849447_story.html?noredirect=on&utm_term=.b9182a13ece1.

[3] ALLIANZ РИСК БАРОМЕТР. Главные риски для бизнеса на 2018 г. URL: https://www.allianz.ru/ru/stuff/%D0%A0%D0%B8%D1%81%D0%BA%20%D0%91%D0%B0%D1%80%D0%BE%D0%BC%D0%B5%D1%82%D1%80%202018.pdf.

Таблиця 5.5

Найбільш значущі ризики для підприємств Європи [4]

Ризики	Місце в рейтингу 2015 р.	Рейтинг 2016 р., %	Рейтинг 2017 р., %	Рейтинг 2018 р., %
Перерва у виробництві та постачанні	1	53	37	42
Ринкові зміни (волатильність, посилення конкуренції, стагнація)	нове	52	31	22
Кіберінциденти (кіберзлочини, витік даних, збої IT)	5	40	30	40
Зміни в законодавстві та регулюванні (економічні санкції, протекціонізм)	4	39	24	21
Макроекономічні зміни (жорстка економія, зростання цін, інфляція)	нове	31	-	-
Природні катастрофи (гроза, повінь, землетрус)	2	31	24	30
Втрата репутації або вартості бренду	7	29	13	13
Пожежа, вибух	3	22	16	20
Нові технології та інновації	нове	19	12	15
Політичні ризики (війна, тероризм, заворушення)	8	17	14	11

Таблиця 5.6

Найбільш значимі ризики для підприємств України

Ризики	Рейтинг 2016 р., %	Місце в рейтингу 2015 р.
Політичні ризики (війна, тероризм, заворушення)	65	1
Розкрадання, шахрайство і корупція	39	2
Тероризм	35	4
Пожежа, вибух	27	3
Перерва у виробництві та постачанні	23	5
Природні катастрофи	15	7
Макроекономічні зміни (жорстка економія, зростання цін, інфляція)	15	8
Єдиний соціальний внесок ринку	15	9
Кіберінциденти (кібератаки, витік даних, збої IT)	15	нове
Зміни в законодавстві та регулюванні (протекціонізм)	12	10

Примітка. Рейтинг складений експертами Редакції Форіншурер http://forinsurer.com/news/16/01/28/33453.

[4] Сьомий Барометр ризиків Allianz є самим масштабним на сьогодні, він складений на основі думок 1911 експертів з 80 країн. Також були опитані консультанти з ризиків, андерайтери, старші керівники та експерти з врегулювання збитків у корпоративному сегменті бізнесу як Allianz Global Corporate & Specialty, так і інших структурних одиниць Allianz. Респонденти опитувались у жовтні – листопаді 2017 року. Респондентів просили вибрати галузі, в яких вони розбираються краще за все, і назвати не більше трьох ризиків, які, на їхню думку, є найбільш важливими. Оскільки можна було відповідати як по одній, так і по двох галузях, і для кожної називати кілька ризиків, було отримано 2376 відповідей, в яких згадувалися 6472 ризики (тому загальна сума не дорівнює 100 %). Більшість відповідей (1257,53 % від загального числа) прийшлось на великі підприємства (з річними надходженнями понад 500 млн €). Середні підприємства (з річними надходженнями від 250 млн € до 500 млн €) подали 516 відповідей (22 %), а малі (з річними надходженнями менше 250 млн €) – 603 відповіді (25 %). В опитуванні брали участь експерти з ризиків із 22 галузей економіки. Зміни в рейтингу Барометра ризиків Allianz визначаються тим, яке місце посідає той чи інший ризик у порівнянні з попереднім роком, а не тим, як змінився відсоток респондентів, що його визначили.

Серед основних причин переривів у виробництві визначені: кіберінциденти – 42 %; пожежі, вибухи – 40 %; стихійні лиха – 39 %; відмови постачальників – 30 %; поломка машин та обладнання – 23 %.

Згідно з даними дослідження, компанії все більше турбує зростаюча витонченість кібератак. Атаки хакерів стають усе більш цілеспрямованими, тривалими і можуть серйозно вплинути на внутрішню діяльність компанії. У міру того як частота і серйозність кібератак зростають, компанії не повинні недооцінювати впливу таких загроз для здійснення діяльності підприємств. Експерти [5] зазначають три основні наслідки кіберінцидентів: перериви у виробництві та порушення ланцюга поставок – 67 %; репутаційні збитки – 52 %; позови про притягнення до відповідальності внаслідок порушення цілісності даних – 45 %.

Можливість зовнішнього і внутрішнього втручання в інформаційну систему підприємства, може вплинути на викривлення таких параметрів інформації, як конфіденційність, цілісність, доступність, достовірність та ін. Це, в свою чергу, може призвести до негативних наслідків у діяльності підприємства [14]:

- збоїв у функціонуванні систем управління технологічними та управлінськими процесами;
- розголошення відомостей, що становлять комерційну та інші види таємниць;
- порушення достовірності фінансової звітності;
- несанкціонованого доступу до бази даних підприємства;
- викривлення публічної інформації.

Результатом викривлення інформації про діяльність підприємства можуть стати:

- зменшення вартості капіталу підприємства;
- труднощі залучення інвестицій;
- розрив (або погіршення) ділових відносин із партнерами;
- зрив переговорів, втрата вигідних контрактів;
- невиконання договірних зобов’язань;
- відмова від рішень, які стали неефективними через розголос інформації;
- втрата можливості запатентувати результат науково-технічної діяльності або продати ліцензію;
- зниження цін або обсягів реалізації;
- завдання шкоди авторитету та діловій репутації фірми;
- більш жорсткі умови отримання кредитів;
- труднощі в постачанні та придбанні устаткування і т. ін.

У певних ситуаціях нехтування питаннями захисту інформації може призвести і до повної втрати бізнесу.

У сьогоднішніх умовах не можна думати про створення інформаційно-аналітичного забезпечення управління економічною безпекою сільськогосподарських підприємств без наукового перегляду фундаментальних основ проце-

[5] Джерело: Allianz Global Corporate & Specialty. Цифри показують відсоток відповідей, в яких названо цей ризик, від загальної кількості відповідей опитаних (857). Цифри не дають у сумі 100 %, оскільки можливо було вибрати до трьох ризиків.

сів управління, реформування яких не може обмежитися деякими оновленням і реконструкцією. На сьогодні потрібна нова парадигма управління як безпосередньо сільськогосподарськими підприємствами, так і їхньою економічною безпекою, параметри якої відповідають умовам і перспективам використання сучасних технологій виробництва сільськогосподарської продукції, зокрема точне землеробство.

Практики і науковці більше ста років розробляють інформаційно-аналітичні інструменти і методи їх використання в практиці прийняття управлінських рішень. Найбільш поширеною сьогодні є концепція пріоритетності значення звітних і прогнозних фінансово-економічних показників, що характеризують ключові аспекти фінансово-господарської діяльності над судженнями про важливість, соціальної й екологічної значущості, що відбуваються в економіці підприємств та в економіці країни.

Перші моделі оцінки результатів діяльності підприємств, що з'явилися в 1920-х роках будуються винятково з фінансових показників, наприклад, мультиплікативна модель Дюпона чи показник рентабельності капіталу ROI.

Перша система фінансових і нефінансових показників оцінки діяльності підприємств, в якій взаємопов'язані інтереси різних зацікавлених сторін (керівників, робітників, постачальників, споживачів та ін.), була сформульована в 1984 р. Р. Фріменом як система показників відповідальності (Accountably Scorecard – ASC) [15]. Ця система знайшла подальший розвиток у концепції збалансованої системи показників (Balanced Scorecard – BSC), розробленої Р. Капланом і Д. Нортоном [16] у 1990 р., яка стала продовженням концепції технології управління за цілями, сформульованої П. Друкером [17].

Суть концепції інформаційно-аналітичного забезпечення управління економічною безпекою сільськогосподарських підприємств повинна формуватися відповідно до застосовуваних методів і способів агрегування інформації, методики побудови показників і їх аналітичної інтерпретації місцезнаходження в системі управління, враховуючи пріоритетність та сукупність факторів, що впливають на успішність реалізації управлінського рішення.

Зростаючий і еволюційний характер кібератак і загроз у комп'ютерних інформаційних системах привели до необхідності пошуку нових підходів і методів захисту інформації. У 1995 році була опублікована стаття керівника дослідницького підрозділу ПВС США Мика Єндслі (Mica Endsley) [18], де було наведено загальне визначення поняття обізнаності про ситуацію, яка описується таким чином: сприйняття елементів середовища в обсязі часу і простору, розуміння їх значення і проектування їхнього стану на майбутнє. Застосування цієї концепції може визивати багато суперечок у сфері управління економічною безпекою, але одним з основних аспектів ситуаційної обізнаності є її динамічність, тобто здатність своєчасно реагувати на нові й мінливі моделі загроз, що прямо суперечать парадигмі класичної економічної безпеки.

Традиційна система економічної безпеки використовує в управлінні ризиками стандартний набір елементів управління для досягнення базового рівня безпеки. Однак у динамічних умовах виникнення загроз слід шукати нові способи і методи моделювання захисту економічних інтересів суб'єктів господа-

рювання, що враховують швидку зміну загроз. Очевидно, що використання концепції «Кібер-усвідомлення ситуації», «Кібер-ситуаційна обізнаність» (Cyber situation awareness) можливе в управлінні економічною безпекою на всіх рівнях економіки.

Сприйняття, розуміння, проекція поточної ситуації та оцінка можливих наслідків і відповідного реагування не може відбутися без людей - аналітики, адміністратори, оператори тощо.

У моделі М. Єндслі представлені три рівня усвідомлення ситуації, сприйняття, розуміння і проекція, пізніше, враховуючи людський фактор і використання концепції ситуаційної обізнаності, Б. Макгінесс [19] та С. Онвубіка (C. Onwubiko) и Т. Оуэнс [20] виділили четвертий рівень – дозвіл. Адаптуючи цю концепцію до управління економічною безпекою підприємства, можна виділити такі рівні усвідомлення ситуації.

Рівень 1. Сприйняття. На цьому рівні аналітики економічної безпеки виявляють можливі вразливі місця в діяльності підприємства та системі управління, це передбачає використання індивідуальних і незалежних інструментаріїв для моніторингу як внутрішнього, так і зовнішнього середовища. На рівні сприйняття, інформація про статус, атрибути й динаміку відповідних загроз як з боку внутрішнього, так і зовнішнього середовища, дозволяє розширити класифікацію загроз у значущі уявлення, які є основою для наступних рівнів: розуміння, проекції і дозволу.

Рівень 2. Розуміння. На цьому рівні аналітики економічної безпеки використовують відповідні інструменти, методи для агрегування, аналізу, узагальнення й зіставлення окремих частин інформаційно-аналітичного забезпечення з метою визначення ризиків та імовірності їх настання. Таким чином, розуміння являє собою сценарій поточної ситуації, який реалізується шляхом визначення значущості отриманих доказів ризиків та загроз, що підлягають моніторингу.

Рівень 3. Проекція. На цьому рівні експерти з питань економічної безпеки прогнозують можливі сценарії розвитку подій. Здатність аналітика зробити точний прогноз на майбутнє може бути підвищена через використання потужних систем моніторингу і технологій, які здатні виявити і передбачити закономірності виникнення майбутніх подій, як приклад, використання системи раннього попередження, що дозволить поліпшити планування і використання профілактичного контролю для запобігання можливих ситуацій.

Рівень 4. Дозвіл. На цьому рівні фахівці з економічної безпеки можуть рекомендувати і здійснювати адекватний контроль і вживати відповідних контрзаходів, необхідні для зменшення чи усунення ризиків, пов’язаних із функціонуванням підприємства.

У новій парадигмі економічна безпека може бути представлена як ситуаційна обізнаність про навколишнє середовище й адекватне реагування на рівень виявленої загрози.

Ситуаційна обізнаність в Economic Security є не який-небудь один продукт – це філософія, яка повинна бути реалізована шляхом розумного використання методів і процесів, які охоплюють економіку підприємства.

Список використаних джерел

1. Виннер Н. Кибернетика и общество. Москва: Издательство иностранной литературы, 1958. 200 с.

2. Словник української мови: в 11 томах. Київ: Наукова думка, 1970. Т. 1: А–В. 799 с.

3. Вербицька Г. Л. Управління економічним ризиком. *Фінанси України*. 2004. № 4. С. 34–41.

4. Великий Ю. М., Проскура О. Ю. Особливості кризового стану вітчизняних підприємств і методів його оцінки. *Фінанси України*. 2002. № 10. С. 29–34.

5. Капустин Н. Экономическая безопасность отрасли и фирмы. *Бизнес Информ*. 1999. № 11. С. 12.

6. Судоплатов А. П., Пекарев С. В. Безопасность предпринимательской деятельности. Москва: ОЛМА-ПРЕСС, 2001. 384 с.

7. Бендиков М. Экономическая безопасность промышленного предприятия (организационно-методический аспект). *Консультант директора*: зб. наук. праць. 2000. № 2. С. 7-13.

8. Сумець О. М., Тумар Б. М. Стратегії сучасного підприємства та його економічна безпека: навч. посіб. Київ: Хай- ТекПрес, 2008. 400 с.

9. Івахненков С. В. Інформаційні технології в організації бухгалтерського обліку та аудиту: навч. посіб. Вид. 4-те, перероб. та доп. Київ: Знання, 2008. 343 с.

10. Ковальов Д., Сухорукова Т. Економічна безпека підприємства. *Економіка України*. 1998. № 11. С. 48–52.

11. Покропивний С. Ф. Економіка підприємства. Київ: КНЕУ 2000. 526 с.

12. Бурячок В. Л., Гулак Г. М., Толубко В. Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: підручник. Київ: ТОВ «СІК ГРУП УКРАЇНА», 2015. 449 с.

13. Nekhai V., Skiter I., Trunova E. Protection of Computer Information Systems of Agricultural Enterprises. *Information Modelsand Analyses.* 2016. Vol. 5, Number 3, P. 246–255.

14. Нехай В. А., Нехай В. В. Інформаційна безпека як складова економічної безпеки підприємств. *Науковий вісник Міжнародного гуманітарного університету. Серія: «Економіка і менеджмент»*. 2017. № 24. С. 137–141.

15. Freeman R. E. Stakeholder Management: A Stakeholder Approach. Marshfield, MA: Pitman Publishing, 1984.

16. Каплан Роберт С., Нортон Дейвид П. Сбалансированная система показателей. От стратегии к действию: пер. с англ. Москва: ЗАО «Олимп-Бизнес», 2003. 214 с.

17. Друкер П. Эффективное управление. Москва:Астрель, 2004. 288 с.

18. Endsley, M.R. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors Journal*. 1995. № 37(1). P. 32–64.

19. McGuinness B. and Foy L. A Subjective Measure of SA: The Crew Awareness Rating Scale (CARS). Proc. of the First Human Performance, Situation Awareness and Automation Conference, Savannah, Georgia, 2000.

20. Onwubiko, C. & Owens T.J. Review of Situational Awareness for Computer Network Defense. In C. Onwubiko and T.J. Owens (Eds.) Situational Awareness in Computer Network Defense: Principles, Methods and Applications. 2011.