УДК 330.131.5:004.065]:339.17

DOI: 10.31617/1.2022(141)08

ЧУБАЄВСЬКИЙ Віталій,
к. політ. н., доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки Державного торговельно-економічного університету
вул. Кіото, 19, м. Київ, 02156, Україна

ORCID: 0000-0001-8078-2652
chubaievskyi_vi@knute.edu.ua

ЖУК Тетяна,
к. е. н., старший викладач кафедри економіки та фінансів підприємства Державного торговельно-економічного університету
вул. Кіото, 19, м. Київ, 02156, Україна

ORCID: 0000-0001-5866-8837
t.zhuk@knute.edu.ua

ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ТОРГІВЛІ

Вступ. *Постійна автоматизація бізнес-процесів, перехід в онлайн-режим під впливом COVID-19 детермінували цифровізацію діяльності підприємств торгівлі. Швидка зміна умов функціонування, аматорська поведінка в інтернет-просторі призвели до стрімкого зростання кіберзлочинів.*

Проблема. *Представники бізнесу дедалі більше усвідомлюють важливість забезпечення достатнього рівня інформаційної безпеки (ІБ). Це, в свою чергу, обумовило необхідність оцінки ефективності, в тому числі економічної, ІБ підприємств торгівлі.*

Метою *статті є обґрунтування необхідності економічної оцінки ефективності інформаційної безпеки як необхідної умови успішної діяльності підприємств торгівлі.*

Методи. *Інформаційну базу дослідження становлять чинні нормативно-правові акти України, публікації вітчизняних та зарубіжних учених з тематики дослідження, матеріали*

CHUBAIEVSKYI Vitalii,
PhD (Politics), Associate Professor, Associate Professor of the Department of Software Engineering and Cyber security
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine

ORCID: 0000-0001-8078-2652
chubaievskyi_vi@knute.edu.ua

ZHUK Tetiana,
PhD (Economics),
Senior Lecturer of the Department of Economics and Business Finance
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine

ORCID: 0000-0001-5866-8837
t.zhuk@knute.edu.ua

ECONOMIC EFFICIENCY OF INFORMATION SECURITY OF TRADE ENTERPRISES

Introduction. *Constant automation of business processes, the transition to online mode under the influence of COVID-19 determined the digitalization of trade enterprises. Rapid changes in operating conditions, amateur behavior in the Internet space have led to a rapid increase in cybercrime.*

Problem. *Businesses are increasingly aware of the importance of ensuring a sufficient level of information security (IS). This, in turn, led to the need to assess the effectiveness, including economic, IS of trade enterprises.*

The aim *of the article is to substantiate the need for economic evaluation of the effectiveness of information security as a necessary condition for the successful operation of trade enterprises.*

Methods. *The information base of the study consists of current regulations of Ukraine, publications of domestic and foreign scientists on the subject of the study, materials of the State Statis-*

© Чубаєвський В., Жук Т., 2022
Внесок авторів є рівнозначним.
Автори не отримували прямого фінансування для цього дослідження.

Chubajevs'kyj V., Zhuk T. Ekonomichna efektyvnist' informacijnoi' bezpeky pidpryjemstv torgivli. *Visnyk Kyi'vs'kogo torgovel'no-ekonomichnogo universytetu*. 2022. №1. S. 106-117. http://doi.org/10.31617/1.2022(141)08

Державної служби статистики України, зарубіжні аналітичні звіти. Використано методи узагальнення, наукового абстрагування та систематизації, аналізу та синтезу, порівняння.

Результати дослідження. *Розкрито сутність понять "інформаційна безпека", "економічна ефективність" у контексті діяльності підприємства. Проаналізовано динаміку капіталовкладень у програмне забезпечення в різних сферах діяльності підприємства. Визначено склад витрат підприємства на забезпечення ефективної системи інформаційної безпеки торговельного підприємства. Досліджено основні методи оцінки економічної ефективності інформаційної безпеки підприємства та визначено найбільш ефективні для підприємств торгівлі.*

Висновки. *Дослідження доводить необхідність оптимізації вартості інформаційного забезпечення. Виявлено особливості вартості інформаційного забезпечення та відокремлення результату (доходу, прибутку) від функціонування ефективної системи інформаційної безпеки. Запропоновано найбільш ефективні методи оцінки економічної ефективності інформаційної безпеки для підприємств торгівлі. Зазначені питання можна поглибити, розглянувши специфіку оцінки економічної ефективності інформаційної безпеки з урахуванням особливостей діяльності оптово-роздрібних підприємств.*

Ключові слова: економічна ефективність, інформаційна безпека, кіберзагрози, кібербезпека, підприємства торгівлі.

tics Service, foreign analytical reports. Methods of generalization, scientific abstraction and systematization, analysis and synthesis, comparison are used.

Results. *The essence of the concepts of "information security", "economic efficiency" in the context of the enterprise is revealed. The dynamics of investment in software in various areas of the enterprise is analyzed. The composition of the company's costs to ensure an effective information security system of a commercial enterprise is determined. The main methods of assessing the economic efficiency of information security of the enterprise are studied and the most effective for trade enterprises are determined.*

Conclusions. *The study proves the need to optimize the cost of information support. The peculiarities of the cost of information support, as well as the peculiarities of the separation of the result (income, profit) from the functioning of an effective information security system are revealed. The most effective methods of assessing the economic efficiency of information security for trade enterprises are proposed. The considered questions can be deepened, having considered specificity of an estimation of economic efficiency of information security taking into account features of activity of wholesale and retail enterprises.*

Keywords: economic efficiency, information security, cyber threats, cybersecurity, trade enterprises.

JEL Classification: M 21, F 19

Вступ. За даними звіту "*Digital* 2021", у січні 2021 р. кількість людей, які користуються інтернетом, збільшилася на 7.3 % порівняно з січнем 2020 р. Зафіксовано загальний рівень користувачів інтернету – близько 59.5 % [1], і ці показники щороку збільшуються, що свідчить про постійне зростання залежності суспільства від інформації та відповідного технологічного середовища. Успішність бізнесу також дедалі більше залежить від вміння обробити інформацію та прийняти відповідні рішення. За даними Державної служби статистики України, кількість підприємств, які мають доступ до мережі інтернет, у 2020 р. порівняно з 2018 р. збільшилася на 1 205 од., а кількість працівників – на 68 324 особи; частка кількості підприємств, що проводили аналіз "великих даних" у 2020 р., порівняно з 2018 р. зросла на 0.2 в. п., а тих, що купують послуги хмарних обчислень, – на 0.4 в. п. [2]. Постійна автоматизація бізнес-процесів, перехід в онлайн-режим під впливом *COVID-19* детермінували цифровізацію діяльності підприємств торгівлі: обсяг реалізованої продукції, отриманий від електронної торгівлі, у 2020 р. відносно 2019 р. збільшився на 24.4 % і на 59.9 % порівняно з 2018 р. [2].

Проблема. Швидка зміна умов функціонування, аматорська поведінка в інтернет-просторі призвели до стрімкого зростання кіберзлочинів. Така ситуація обумовила збільшення витрат підприємств на навчання у сфері ІКТ: як свідчать статистичні дані, частка кількості таких підприємств зросла на 0.8 в. п. для фахівців у сфері ІКТ і на 0.3 в. п. – для інших працівників [2]. Тобто представники бізнесу дедалі більше усвідомлюють важливість забезпечення достатнього рівня інформаційної безпеки (ІБ). Це, в свою чергу, обумовило необхідність оцінки ефективності, в тому числі економічної, ІБ підприємств торгівлі.

Аналіз останніх досліджень і публікацій. Результати дослідження державного та галузевого аспектів питань ІБ висвітлено у працях таких науковців, як: Л. Рибальченко, Е. Рижков, С. Тютченко, О. Гавриш, А. Варяниченко, К. Фокіна-Мезенцева, М. Нежива, В. Мисюк [3–5]. В. Панченко розглядав ІБ підприємства як складову загальної інформаційної безпеки держави [6]. І. Аванесова, Г. Азаренкова, А. Майборода, В. Бакай, В. Зима, Л. Бехтер, К. Утенкова дослідили окремі аспекти ІБ за галузями діяльності підприємств [7–11].

Крім того, у працях зазначених учених розглянуто окремі проблеми ефективності ІБ. Проте з підвищенням ролі інформації у діяльності підприємств торгівлі (ПТ) актуалізується питання оцінки саме економічної ефективності.

Мета статті – обґрунтування необхідності економічної оцінки ефективності інформаційної безпеки як необхідної умови успішного функціонування підприємств торгівлі.

Методи. Для досягнення основної мети дослідження застосовано методи узагальнення, наукового абстрагування та систематизації, аналізу та синтезу, порівняння. Інформаційну базу дослідження становлять чинні нормативно-правові акти України, публікації вітчизняних та зарубіжних науковців за темою дослідження, матеріали Державної служби статистики України, зарубіжні аналітичні звіти.

Результати дослідження. У Законі України "Про інформацію" наведено визначення поняття "захист інформації" [12], яке є вужчим порівняно з поняттям "інформаційна безпека". *Інформаційна безпека* охоплює процеси не тільки захисту інформації, але й, наприклад, обміну інформацією. У Законі України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" ІБ визначається як "стан захищеності" [13]. Визначення, наведене у цьому Законі, має загальний характер і розкриває зміст ІБ загалом для суспільства, держави, окремої особистості. Дещо інше визначення надає О. Сороківська: "ІБ – суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності" [14], акцентуючи на змісті цього поняття для суб'єктів господарювання, визначивши його як "суспільні відносини". Саме така сутнісна характеристика ІБ підкреслює, що суб'єкти господарювання функціонують у системі, яка передбачає взаємодію з іншими суб'єктами суспільства.

Поняття *ефективності*, в тому числі *економічної* розглянуто у працях багатьох вітчизняних і закордонних учених. Зміст терміна "ефективність" зводиться до відношення результату (ефекту) до витрат, "економічну ефективність" розглядають як різновид ефективності, що передбачає досягнення найбільших результатів за найменших витрат. З огляду на це, *економічна ефективність інформаційної безпеки підприємства* зводиться до визначення основних параметрів: *результату* та *витрат*.

Традиційні методи не дають змоги обробити стрімкі потоки інформації, проаналізувати динамічні зміни у системі господарювання. Це обумовлює використання інформаційних технологій для обміну, збереження, обробки, аналізу інформації. У зв'язку з цим доречно більшу увагу приділити цифровій безпеці підприємства, ніж фізичному захисту інформації.

Аналіз витрат на забезпечення інформаційної безпеки підприємств торгівлі (ІБПТ) доцільно розпочати з витрат підприємств різних видів економічної діяльності на програмне забезпечення (ПЗ), які складаються з: придбання антивірусних програм, що обумовлює захист інформації; специфічних програм галузі (наприклад, у сфері торгівлі програми пов'язані із закупівлею, обробкою та доставкою замовлень); програми, які є допоміжними у забезпеченні основного виду діяльності (наприклад, фінансові, бухгалтерські тощо).

Для з'ясування рівня ІБПТ у межах країни необхідно провести порівняльний аналіз капітальних витрат на ПЗ за видами економічної діяльності.

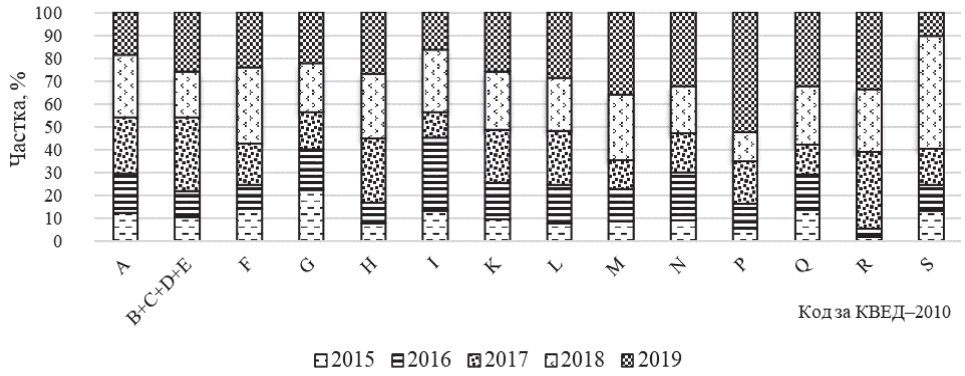

Рис. 1. Частка капітальних інвестицій у програмне забезпечення в загальному обсягу по підприємствах за видами економічної діяльності у 2015–2019 рр.

Джерело: побудовано авторами за даними [2].

Результати аналізу даних *рис. 1* показують, що по всіх видах економічної діяльності частка інвестицій у ПЗ упродовж 2018–2019 рр. становила близько 50 % на противагу 2015–2017 рр. Це свідчить про поступове нарощування темпів зростання обсягів інвестицій. У сфері

освіти (*P*) більше ніж 50 % від загальної суми інвестицій за 2015–2019 рр. припадає саме на 2019 р. Суттєві зрушення спостерігаються й у сфері професійної та наукової діяльності (*M*), де більше 30 % від усього розміру капітальних інвестицій у ПЗ упродовж аналізованого періоду припали на 2019 р. Найменше у 2019 р., на противагу попереднім періодам, інвестовано у ПЗ підприємствами таких сфер, як: надання інших видів послуг, тимчасове розміщення та організація харчування (*S* та *I* відповідно).

Більш детальну характеристику за обсягами капітальних інвестицій у ПЗ наведено у *табл. 1*.

Таблиця 1

Капітальні інвестиції підприємств у програмне забезпечення за видами економічної діяльності у 2015-2019 рр.

Вид економічної діяльності, КВЕД	Обсяг, млн грн					Темпи приросту, %	
	2015	2016	2017	2018	2019	2019/2018	2019/2015
Сільське, лісове, рибне господарства, *A*	25.56	36.92	50.95	58.13	39.23	–32.52	53.44
Промисловість, *B+C+D+E*	637.27	696.03	1955.74	1220.69	1589.92	30.25	149.49
Будівництво, *F*	16.72	12.39	21.89	39.43	28.72	–27.17	71.72
Оптова та роздрібна торгівля; ремонт автотранспортних засобів і мотоциклів, *G*	849.24	684.07	635.92	820.99	858.56	4.58	1.10
Транспорт, складське господарство, поштова та кур'єрська діяльність, *H*	108.92	126.66	400.69	398.63	380.06	–4.66	248.95
Тимчасове розміщування й організація харчування, *I*	10.44	25.50	8.82	21.84	13.25	–39.35	26.90
Фінансова та страхова діяльність, *K*	31.80	53.46	77.79	85.60	86.69	1.27	172.59
Операції з нерухомим майном, *L*	16.80	35.86	51.66	49.96	62.76	25.62	273.53
Професійна, наукова та технічна діяльність, *M*	81.07	133.79	120.13	268.97	340.92	26.75	320.51
Діяльність у сфері адміністративного та допоміжного обслуговування, *N*	51.49	120.28	99.98	118.84	185.89	56.43	261.01
Освіта, *P*	1.54	3.18	5.39	3.77	15.23	304.11	892.25
Охорона здоров'я та надання соціальної допомоги, *Q*	14.18	16.15	13.97	26.55	34.10	28.43	140.39
Мистецтво, спорт, розваги та відпочинок, *R*	0.33	0.67	6.02	5.00	6.06	21.36	1753.82
Надання інших видів послуг, *S*	0.89	0.77	1.07	3.34	0.72	–78.54	–19.46

Джерело: складено авторами на основі даних [2].

Як випливає з *табл. 1*, найбільше капітальних інвестицій у ПЗ вкладено підприємствами промисловості, що пов'язано з високим рівнем капіталовкладень галузі загалом та постійним удосконаленням процесів, автоматизацією виробничих потужностей підприємств. Наведені дані свідчать про постійну тенденцію зростання обсягів інвестицій упродовж 2015–2019 рр. Наступний вид економічний діяльності за найбільшими обсягами інвестицій – оптова та роздрібна торгівля, ремонт автотранспортних засобів і мотоциклів. Незначний темп приросту розміру інвестицій порівняно з 2015 р. обумовлений його зменшенням у 2016–2017 рр. Значний обсяг інвестицій у ПЗ підприємств цієї сфери визначений найбільшою кількістю суб'єктів господарювання, розвитком онлайн-торгівлі. Найбільший темп зростання в аналізований період продемонстрували мистецтво, спорт, розваги та відпочинок. Причиною стрімкого зростання став розвиток онлайн-розваг, перехід креативних індустрій у режим онлайн.

Для подальшого належного рівня забезпечення ІБ в Україні необхідно підтримувати інвестування в освіту, професійну, наукову та технічну діяльність: від рівня освіти фахівців сфери ІТ напряму залежить ІБ підприємств; сфера ж професійної, наукової, технічної діяльності безпосередньо формує науковий потенціал країни, в тому числі є базою для створення відповідного ПЗ. І освіта (див. *табл. 1*), продемонструвала вибухові зрушення в обсягах інвестування у ПЗ. Тенденція зростання цього показника у сфері професійної, наукової, технічної діяльності значно скромніша, але також виглядає оптимістично.

За даними, наведеними у звіті *Verizon Data Breach Investigations Report* за 2020 р., 99 % кібератак, що здійснені на підприємства торгівлі, мали фінансовий мотив. Серед виявлених 725 інцидентів підтверджено лише 165, але, як зазначають автори звіту, близько 405 непідтверджених інцидентів – це DDoS-атаки. Крім того, ритейл визнано одним з ключових секторів атак зловмисників. Найбільш розповсюдженими видами атак у ритейлі стали: системні вторгнення та соціальний інжиніринг, частка яких становить близько 60 % від загального обсягу кібератак у ритейлі. Системні вторгнення пов'язані з неавторизованим доступом до мережі, які не ідентифікують антивірусні програми. Виявляються такі інциденти, зазвичай, постфактум. Соціальний інжиніринг у вигляді застосування *Pretexting* притаманний саме сфері ритейлу. *Pretexting* становить близько 60 %, фішинг – 40 % від загальної кількості соціальних моделей кібератак. Тип інформації, на який були найбільше націлені зловмисники, – це інформація щодо платіжних карток клієнтів. Крім того, особисті й облікові дані є привабливими для фінансових зловмисників – саме вони є цінним об'єктом кібератак [15].

Під впливом *COVID-19* активно розвивалася онлайн-сфера бізнесу. Торговельні підприємства не стали винятком, у зв'язку з чим підвищився рівень кіберзагроз. Кіберзагрози для ПТ пов'язані з шифруванням або викраденням даних клієнтів, уповільненням торговельних процесів. Це, в свою чергу, призводить до значних витрат підприємства. Натомість за умови успішної кібератаки вартість цифрової безпеки ПТ суттєво збільшиться, а втрати включатимуть не тільки оголошений викуп за викрадену або зашифровану інформацію.

Вартість *цифрової безпеки* підприємств торгівлі складається з витрат на запобігання кібератак (програмне забезпечення; навчання цифровій грамотності працівників; організація системи безпеки, мотиваційної політики та корпоративної культури). Ціною ж *вразливості* будуть витрати на ліквідацію наслідків від кібератак (викуп, відновлення операційних процесів, репутації тощо).

Втрати торговельного підприємства у випадку успішної кібератаки матимуть негативний вплив як на фінансовий стан підприємства, так і на його подальші перспективи розвитку у конкурентному середовищі.

По-перше, це *грошові втрати* ТП, пов'язані з уповільненням темпів зростання товарообороту і, як наслідок, недоотримання доходів і прибутку у найближчій та середньостроковій перспективі.

По-друге, якщо кібератака зловмисників мала успіх, найчастіше це призводить до втрати *репутації*. Найбільш критично це для відомих брендів, які мають певну репутацію, що створювалася роками, їм довіряють клієнти і працівники. При порушенні ж ІБ конфіденційні дані потрапляють до зловмисників, що руйнує довіру. І навіть швидка реакція з боку компанії – своєчасний викуп або дешифрування даних, стрімке відновлення основних процесів – не повертає клієнтам комфорту і відчуття впевненості. Втрата довіри призводить до скорочення обсягів покупок в очікуванні розвитку подій, часткової втрати постійних клієнтів, стає значною перешкодою для залучення нових. Це, в свою чергу, обумовлює зниження конкурентоспроможності ПТ.

По-третє, незалежно від того, яке рішення приймають керівники компаній – задоволення вимог зловмисників або самостійне вирішення проблем, – ці процеси супроводжуються *втратою часу*, який є дедалі ціннішим ресурсом будь-якого бізнесу в умовах прискорення розвитку інформаційного суспільства. Відволікання грошових коштів, втрата фінансових можливостей, як наслідок – втрата мобільності при змінному попиті суттєво знижує конкурентні можливості підприємства.

По-четверте, викрадення *бази даних* зловмисниками може бути пов'язане не тільки з особистими даними клієнтів, але й з конфіденційною інформацією підприємства торгівлі. Оприлюднення цих даних призведе до втрати конкурентних переваг компанії. Конфіденційна інформація контрагентів також опиняється під загрозою оприлюднення, що, в свою чергу, призводить до штрафів, санкцій, судових витрат.

По-п'яте, викрадення, шифрування даних зумовлює *порушення бізнес-процесів* ПТ. Але не менш важливим є пошкодження і втручання в закупівельні, збутові та інші бази за видами діяльності підприємства, що може супроводжуватися іншою формою кіберзагрози, наприклад, вірусною атакою. Тимчасова втрата доступу до платіжної системи банку, бухгалтерських, кур'єрських програм та іншого призводить до тимчасової дезорієнтації і уповільнення торговельних бізнес-процесів. І, як наслідок – зниження обсягу товарообороту та інших ключових показників діяльності підприємства.

По-шосте, відносини з *інвесторами*. Зазвичай, великі торговельні мережі, особливо міжнародного рівня, при ліквідації наслідків кібератаки не втрачають своїх інвесторів або акціонерів – це пов'язано з достатньою кількістю фінансових ресурсів і наявністю потужної системи інформаційної безпеки. Але, якщо йдеться про середні за розміром підприємства, в яких недосконала система безпеки і які потребують додаткових вкладень з боку інвесторів (акціонерів) для подальшого розвитку, то після успішної кібератаки існує висока ймовірність втрати довіри інвестора (акціонера) такими підприємствами та/або обмеження можливостей залучення інших інвесторів (акціонерів) для подальшого розвитку.

Результат (ефект) ІБПТ сучасні автори розраховують через темпи зміни доходу (прибутку), відвернений збиток. Обчислення обох показників є складним. Методику розрахунку темпів зміни доходу (прибутку)

можна поділити на 2 підходи через розрахунок: приросту доходу (прибутку); недоотриманої суми доходу (прибутку). Розрахунок приросту доходу (прибутку) залежить від наявності достатнього рівня ІБ і ускладнений тим, що фактично система ІБ є не центром формування прибутку, а допоміжною в загальній системі підприємства. Крім того, достатній (належний) рівень розрахунку критерію ІБ підприємства вимагає своєї системи оцінки. Недоотримана сума доходу (прибутку) може розраховуватися через імовірність настання кібератаки або є результатом фактичної кібератаки. Розрахунок показника ймовірності настання кібератаки ускладнений тим, що кібератаки не мають певної системи. Фактичні додаткові витрати підприємства для викупу інформації, відновлення бізнес-процесів після кібератаки і порівняння фактичних значень доходу (прибутку) із запланованими є основними показниками для розрахунку економічної ефективності у випадку успішної кібератаки.

Методика розрахунку результату (ефекту) через відвернений збиток передбачає аналіз усіх інформаційних загроз, яким піддавалося підприємство протягом певного часу, де враховується можлива вартість викупу на відновлення бізнес-процесів. У цьому випадку економічна ефективність розраховується як зіставлення суми відверненого збитку з витратами підприємства на організацію належного рівня ІБ.

Сучасні методики, які використовуються для оцінки економічної ефективності, представлено у *табл. 2*.

Таблиця 2

Методики оцінки економічної ефективності інформаційної безпеки підприємств торгівлі

Назва методики	Оптимізація витрат	Визначення результату	Максимізація результату	Оцінка ризиків	Розроблення ймовірних сценаріїв
Прикладний інформаційний аналіз (*Applied Information Economics, AIE*)	+	+	–	+	+
Споживчий індекс (*Customer Index, CI*)	–	+	–	–	–
Додана економічна вартість (*Economic Value Added, EVA*)	–	+	–	–	–
Вихідна економічна вартість (*Economic Value Sourced, EVS*)	–	+	+	+	+
Управління портфелем активів (*Portfolio Management, PM*)	+	+	+	+	+
Оцінка дійсних можливостей (*Real Option Valuation, ROV*)	+	+	+	+	+
Метод життєвого циклу штучних систем (*System Life Cycle Analysis, SLCA*)	–	+	–	+	+
Система збалансованих показників (*Balanced Scorecard, BSC*)	+	+	+	–	–
Сукупна вартість володіння (*Total Cost of Ownership, TCO*)	+	–	–	–	–
Функціонально-вартісний аналіз (*Activity Based Costing, ABC*)	+	–	–	–	+
Метод експертних оцінок	–	+	–	+	–

Джерело: систематизовано авторами за [16–18].

Дані *табл. 2* відображають можливість кожної з методик визначати складові економічної ефективності ІБ. З огляду на сутність економічної ефективності, передусім необхідно звернути увагу на мето-

дики, які дають змогу оптимізувати (мінімізувати) витрати на ІБ. *AIE* передбачає оцінку ефективності інвестицій у технології безпеки з використанням експортних оцінок якісних показників. У такому випадку важливу роль відіграють особисті якості експертів (знання, досвід). Використання *AIE* доволі складне і вимагає звернення до компанії-консультанта. Застосування методики *PM* надає можливість оптимізувати витрати у режимі реального часу, але оцінка і прийняття рішень покладені на керівника і залежать від його особистих якостей. Метод *ROV* є трудомісткім і обмеженим у використанні, застосовується на стадії проєктування. Застосування *BSC* передбачає розроблення унікальних критеріїв: залежно від стратегії підприємства, показників оцінки задаються планові значення показників. Через те, що ІБ є допоміжною системою, виникає ряд проблем у побудові збалансованої моделі. Стратегічні показники підприємства стосовно основної діяльності необхідно пов'язати з показниками інформаційної безпеки. *ABC*-метод, орієнтований на виробничу та логістичну систему підприємства, пов'язаний з визначенням і розподілом витрат.

За результатами аналізу можливостей розглянутих методів визначення розміру витрат і результату, оцінки економічної ефективності зроблено такі висновки:

- застосування деяких методів є неможливим для мікропідприємств торгівлі, що пов'язано з їх значною трудомісткістю, відсутністю експертів тощо;
- метод *Customer Index* найбільше відображає специфіку діяльності ПТ і дає змогу оцінити вплив інвестицій в ІБ на динаміку кількості споживачів;
- використання методу *Total Cost of Ownership* надає найбільше можливостей аналізу і мінімізації витрат на підприємстві, але для визначення результату необхідно застосовувати принаймні ще одну методику;
- наведені методи базуються на аналізі даних попередніх періодів (сталого розвитку) та під впливом пандемії *COVID-19* і пов'язаних з цим карантинних обмежень прогнозні дані виявилися помилковими.

Сучасні реалії змусили розробників звернути увагу на інші способи дослідження. Наразі йдеться про аналіз емоцій споживачів. Під час *аналізу поведінки споживача* експертами з'ясовано, що, обираючи товар, вони керуються не раціональним вибором, а емоціями [19]. Інструменти текстового аналізу на основі штучного інтелекту (*Clarabridge* і *IBM Watson)* підвищують точність інструментів аналізу настроїв, у той час як такі фірми, як *Nielsen* і *Realeyes*, переносять методи біометричного і фейс-аналізу у бізнес.

Таким чином, використання певної методики під час оцінки економічної ефективності ІБПТ передусім обумовлено характером діяльності, розміром підприємства, наявністю інтернет-продажів, цілей.

Висновки. Оскільки підприємства торгівлі є провідною ланкою між виробничими підприємствами і споживачами, то вони найбільш чутливі до зміни потреб і бажань суспільства. Саме підприємства торгівлі

найбільш вразливі для кіберзагроз: їх специфіка у тому, що основною метою є задоволення попиту на товари, а не захист інформації. Проведене дослідження доводить необхідність оптимізації витрат на інформаційне забезпечення. Виявлено особливості складу витрат на інформаційне забезпечення, а також особливості виокремлення результату (доходу, прибутку) від функціонування ефективної системи інформаційної безпеки. Визначено найбільш результативні методики оцінки економічної ефективності інформаційної безпеки для підприємств торгівлі.

Розглянуті питання можна поглибити, проаналізувавши специфіку оцінки економічної ефективності інформаційної безпеки з урахуванням особливостей діяльності оптових і роздрібних підприємств.

Конфлікт інтересів. Автори заявляють, що вони не мають фінансових чи нефінансових конфліктів інтересів щодо цієї публікації; не мають відносин із державними органами, комерційними або некомерційними організаціями, які могли б бути зацікавлені у поданні цієї точки зору. З огляду на те, що автори працюють в установі, яка є видавцем журналу, що може зумовити потенційний конфлікт або підозру в упередженості, остаточне рішення про публікацію цієї статті (включно з вибором рецензентів та редакторів) приймалося тими членами редколегії, які не пов'язані з цією установою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Digital 2021 global overview report. URL: https://www.hootsuite.com/resources/digital-trends.
2. Статистична інформація Державної служби статистики України. URL: http://www.ukrstat.gov.ua/operativ/oper_new.html.
3. Рибальченко Л. В., Рижков Е. В., Тютченко С. М. та ін. Безпека підприємництва: монографія. Дніпро: Видавець Біла К. О., 2020. 180 с.
4. Фокіна-Мезенцева К. Інформаційна безпека у глобальному суспільстві. *Вісник Київ. нац. торг.-екон. ун-ту.* 2021. № 5. С. 61-71. http://doi.org/10.31617/visnik.knute.2021(139)04.
5. Нежива М., Мисюк В. ASP Structure: prevention of economic fraud. *Вісник Київ. нац. торг.-екон. ун-ту.* 2021. № 1. С. 41-52. http://doi.org/10.31617/visnik.knute.2021(135)03.
6. Панченко В. Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти. *Актуальні проблеми правознавства.* 2020. № 1(21). С. 103-109.
7. Аванесова І. Інформаційна безпека у системі захисту прав споживачів фінансових послуг. *Вісник Київського національного торговельно-економічного університету.* 2018. № 2. С. 55-66. URL: http://visnik.knute.edu.ua/files/2018/02/6.pdf.
8. Азаренкова Г. М., Майборода А. В. Особливості формування підсистеми інформаційного забезпечення системи фінансової безпеки суб'єкта господарювання. *Бізнес Інформ*. 2020. №1. С. 210-217. http://doi.org/10.32983/2222-4459-2020-1-210-217.
9. Бакай В. Й., Зима В. М. Нові виклики та особливості створення системи інформаційної безпеки підприємства. *Вісник Хмельницького національного університету.* 2020. № 5. С. 19-22.
10. Бехтер Л. А. Загрози інформаційної безпеки та захист інформації як складова економічної безпеки сільськогосподарських підприємств. *Агросвіт.* 2020. № 12. С. 66-70. http://doi.org/10.32702/2306-6792.2020.12.66.
11. Утенкова К. О. Теоретичні засади формування методики експертної оцінки впливу окремих чинників на стан економічної безпеки аграрних підприємств. *Економіка та держава*. 2020. № 4. С.133-140. http://doi.org/10.32702/ 2306-6806.2020.4.133.
12. Про інформацію: Закон України від 02.10.92 № 2657-XII. Дата оновлення: 16.07.2020. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 20.10.2021).
13. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V. Дата оновлення: 06.02.2007. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення 20.10.2021).

14. Сороківська О. А., Шведа Н. М. Інформаційна безпека підприємства в умовах застосування бенчмаркінгу. *Регіональна бізнес-економіка та управління*. 2013. № 2. С. 55-61.
15. Data Breach Investigations Report 2020. URL: https://www.verizon.com/business/resources/reports/dbir (дата звернення 20.10.2021).
16. An Overview of Applied Information Economics. URL: https://hubbardresearch.com/about/applied-information-economics (дата звернення 20.11.2021).
17. Customer intelligence. URL: https://searchcustomerexperience-techtarget-com.translate.goog/definition/customer-intelligence-CI?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=uk&_x_tr_pto=op,sc (дата звернення 20.11.2021).
18. A mathematical model of information security for a mining company. E3S Web Conf. Vth International Innovative Mining Symposium. 2020. Vol. 174. URL: https://www.e3s-conferences.org/articles/e3sconf/abs/2020/34/e3sconf_iims2020_04012/e3sconf_iims2020_04012.html.
19. Predictions 2021: Customer Insights Practices Continue To Evolve. URL: https://www.forrester.com/blogs/customer-insights-2021-predictions (дата звернення 20.10.2021).

REFERENCES

1. Digital 2021 global overview report. *www.hootsuite.com*. https://www.hootsuite.com/resources/digital-trends [in English].
2. Statystychna informacija Derzhavnoi' sluzhby statystyky Ukrai'ny [Statistical information of the State Statistics Service of Ukraine]. *www.ukrstat.gov.ua.* http://www.ukrstat.gov.ua/operativ/oper_new.html [in Ukrainian].
3. Rybal'chenko, L. V., Ryzhkov, E. V., Tjutchenko, S. M. et al. (2020). *Bezpeka pidpryjemnyctva [Business security]*. Dnippo: Vydavec' Bila K. O. [in Ukrainian].
4. Fokina-Mezenceva, K. (2021). Informacijna bezpeka u global'nomu suspil'stvi [Information security in the global society]. *Visnyk Kyi'vs'kogo nacional'nogo torgovel'no-ekonomichnogo universytetu – Herald of Kyiv National University of Trade and Economics, 5*, 61-71. http://doi.org/10.31617/visnik.knute.2021(139)04 [in Ukrainian].
5. Nezhyva, M., & Mysjuk, V. (2021). ASP Structure: prevention of economic fraud. *Visnyk Kyi'vs'kogo nacional'nogo torgovel'no-ekonomichnogo universytetu – Herald of Kyiv National Universityof Trade and Economics, 1*, 41-52. http://doi.org/10.31617/visnik.knute.2021(135)03 [in Ukrainian].
6. Panchenko, V. (2020). Upravlinnja informacijnoju bezpekoju derzhavy ta pidpryjemstv: pravovi ta organizacijni aspekty [Management of information security of the state and enterprises: legal and organizational aspects]. *Aktual'ni problemy pravoznavstva – Current Issues of Jurisprudence, 1 (21)*, 103-109 [in Ukrainian].
7. Avanesova, I. (2018). Informacijna bezpeka u systemi zahystu prav spozhyvachiv finansovyh poslug [Information security in the system of protection of the consumers rights of financial services]. *Visnyk Kyi'vs'kogo nacional'nogo torgovel'no-ekonomichnogo universytetu – Herald of Kyiv National University of Trade and Economics, 2*, 55-66. http://visnik.knute.edu.ua/files/2018/02/6.pdf [in Ukrainian].
8. Azarenkova, G. M., & Majboroda, A. V. (2020). Osoblyvosti formuvannja pidsystemy informacijnogo zabezpechennja systemy finansovoi' bezpeky sub'jekta gospodarjuvannja [Formation features of the information support subsystem of the financial security system of the business entity]. *Biznes Inform – Business Inform*, *1*, 210-217. http://doi.org/10.32983/2222-4459-2020-1-210-217 [in Ukrainian].
9. Bakaj, V. J., & Zyma, V.M. (2020). Novi vyklyky ta osoblyvosti stvorennja systemy informacijnoi' bezpeky pidpryjemstva [New challenges and features of creating an information security system of the enterprise]. *Visnyk Hmel'nyc'kogo nacional'nogo universytetu – Bulletin of Khmelnytskyi National University, 5*, 19-22 [in Ukrainian].

10. Behter, L. A. (2020). Zagrozy informacijnoi' bezpeky ta zahyst informacii' jak skladova ekonomichnoi' bezpeky sil's'kogospodars'kyh pidpryjemstv [Information security threats and information protection as a component of economic security of agricultural enterprises]. *Agrosvit – Agrosvit, 12*, 66-70. http://doi.org/10.32702/2306-6792.2020.12.66 [in Ukrainian].
11. Utenkova, K. O. (2020). Teoretychni zasady formuvannja metodyky ekspertnoi' ocinky vplyvu okremyh chynnykiv na stan ekonomichnoi' bezpeky agrarnyh pidpryjemstv [Theoretical bases of formation technique of an expert estimation of influence of separate factors on a condition of economic safety of the agrarian enterprises]. *Ekonomika ta derzhava – Economy and State*, *4*, 133-140. http://doi.org/10.32702/2306-6806.2020.4.133 [in Ukrainian].
12. Pro informaciju Zakon Ukrai'ny vid 02.10.92 № 2657-XII. Data onovlennja: 16.07.2020. [The Law of Ukraine "On Information" dated 02.10.1992 No. 2657-XII. Updated date: 16.07.2020]. https://zakon.rada.gov.ua/laws/show/2657-12#Text (acessed on 20 October 2021) [in Ukrainian].
13. Pro Osnovni zasady rozvytku informacijnogo suspil'stva v Ukrai'ni na 2007-2015 roky: Zakon Ukrai'ny vid 09.01.2007 № 537-V. Data onovlennja: 06.02.2007 [Law of Ukraine "On the Basic Principles of Information Society Development in Ukraine for 2007-2015" dated 09.01.2007 No. 537-V. Updated date: 06.02.2007]. https://zakon.rada.gov.ua/laws/show/537-16#Text (accessed on 20 October 2021) [in Ukrainian].
14. Sorokivs'ka, O. A., & Shveda, N. M. (2013). Informacijna bezpeka pidpryjemstva v umovah zastosuvannja benchmarkingu [Enterprise information security in the conditions of application of benchmarking]. *Regional'na* biznes-ekonomika ta upravlinnja – *Regional Business Economics and Management, 2*, 55-61 [in Ukrainian].
15. Data Breach Investigations Report (2020). https://www.verizon.com/business/resources/reports/dbir (accessed on 20 October 2021) [in English].
16. An Overview of Applied Information Economics. *hubbardresearch.com*. https://hubbardresearch.com/about/applied-information-economics (accessed on 20 November 2021) [in English].
17. Customer intelligence. *searchcustomerexperience-techtarget-com.translate.goog*. https://searchcustomerexperience-techtarget-com.translate.goog/definition/customer-intelligence-CI?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=uk&_x_tr_pto=op,sc (accessed on 20 November 2021) [in English].
18. A mathematical model of information security for a mining company (2020). E3S Web Conf. Vth International Innovative Mining Symposium. Vol. 174. https://www.e3s-conferences.org/articles/e3sconf/abs/2020/34/e3sconf_iims2020_04012/e3sconf_iims2020_04012.html [in English].
19. Predictions (2021). Customer Insights Practices Continue To Evolve. https://www.forrester.com/blogs/customer-insights-2021-predictions (accessed on 20 October 2021) [in English].

Надійшла до редакції 01.12.2021.
Прийнято до друку 20.12.2022.
Публікація онлайн 24.02.2022.