УДК 657.1.011.56:631.15-049.5

JEL classification: M41, B52

DOI: https://doi.org/10.35774/visnyk2021.01.097

Станіслав ВАСИЛІШИН,
доктор економічних наук, доцент,
завідувач кафедри бухгалтерського обліку і аудиту,
Харківський національний аграрний університет ім. В. В. Докучаєва,
учбове містечко ХНАУ, селище Докучаєвське,
Харківська область, 62483, Україна,
e-mail: vasylishynstanislav@gmail.com
ORCID ID: 0000-0001-5023-9878

УДОСКОНАЛЕННЯ ВАЖЕЛІВ УПРАВЛІННЯ ДІДЖИТАЛІЗАЦІЙНИМИ РИЗИКАМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТА ФОРМУВАННЯ КІБЕРБЕЗПЕКИ ОБЛІКОВОЇ СИСТЕМИ

Василішин С. Удосконалення важелів управління діджиталізаційними ризиками економічної безпеки та формування кібербезпеки облікової системи. *Вісник економіки.* 2021. Вип. 1. С. 97–110. DOI: https://doi.org/10.35774/visnyk2021.01.097

Vasylyshyn S. (2021). Improving the levers of digitalization risks management of economic security and formation of cybersecurity of the accounting system. *Visnyk economiky – Herald of Economics, 1,* 97–110. DOI: https://doi.org/10.35774/visnyk2021.01.097

Анотація

Вступ. *XXI ст. – ера інформаційного суспільства, яка радикально змінила умови життя і розвитку суб'єктів бізнесу. Саме тому нині стрімко розвивається окремий напрямок економічних досліджень, пов'язаний з розробкою заходів щодо зміцнення економічної безпеки підприємств у діджиталізованому світі.*

Мета дослідження *полягає в оцінюванні стану та розробці шляхів удосконалення важелів управління діджиталізаційними ризиками економічної безпеки і формування кібербезпеки облікової системи підприємств.*

Методи. *Для досягнення визначеної мети використано різні методи та прийоми: системного підходу (розробка адаптивної системи забезпечення кібербезпеки як функції служби економічної безпеки підприємства); аналізу і синтезу (визначення діджиталізаційних ризиків та характеру їх впливу на обліково-аналітичне забезпечення); монографічний (ідентифікація компонент інформаційної безпеки). З метою глибокого аналізу поглядів професійного середовища на окремі аспекти обліково-аналітичного забезпечення економічної безпеки в цифровому світі проведено всеукраїнське експертне опитування – анкетування працівників бухгалтерських служб, науковців та здобувачів освітніх ступенів «Місце*

© Станіслав Василішин, 2021.

економічної безпеки в системі обліково-аналітичного забезпечення управління підприємствами і трансформація бухгалтерської професії в цифровому світі», що тривало протягом 2019–2020 рр. і охопило 858 респондентів, серед яких 62,1 % становлять бухгалтери-практики провідних підприємств Східної України. У процесі експертного опитування розроблено методику анкетування безповторної типової вибірки респондентів. Оскільки у вибіркову сукупність у тій чи іншій пропорції, обов'язково потрапили представники всіх груп, типізація генеральної сукупності дозволила виключити вплив міжгрупової дисперсії на середню помилку вибірки, яка в цьому випадку визначається тільки внутрішньо-груповою варіацією.

***Результати.** Проаналізовано структуру та типи основних правопорушень у галузі кібербезпеки українських підприємств. На основі результатів всеукраїнського експертного опитування-анкетування бухгалтерів визначено вагомість окремих груп та структуру діджиталізаційних ризиків обліково-аналітичного забезпечення. Розкриті технічний, програмний, інформаційний, кадровий та організаційний компоненти інформаційної безпеки підприємств. Розроблена адаптивна система забезпечення кібербезпеки підприємства на основі виокремлення експертної групи з інформаційної безпеки, яка є складовою служби економічної безпеки і виконує функції моніторингу кіберзагроз, координації тактичних дій та формування стратегій кіберзахисту підприємств або залучення послуг IT-компаній інтеграторів. На основі моделювання заходів із реагування та нівелювання кіберзагроз інформаційної безпеки на різних стадіях кібератак запропоновано реалізацію попереджувального, реакційного, захисного і прогностично-моніторингового етапів кіберзахисту.*

***Перспективи.** Потенційний успіх підприємства в умовах трансформаційних змін економіки у процесі діджиталізації прямо залежатиме від зміни бухгалтерської парадигми, яка є основним елементом модифікацій щодо бізнес-процесів, і головним джерелом задоволення інформаційних потреб усіх груп стейкхолдерів, пов'язаних з економічною безпекою підприємницьких структур.*

К***лючові слова:*** *діджиталізація, економічна безпека, кібербезпека, діджиталізаційні ризики, облікова система, підприємство.*

Формули: 0, рис.: 5, табл.: 2, бібл.: 12.

Stanislav VASYLISHYN,
Ds (Economics), Associate Professor,
Head of the Department of Accounting and Auditing,
Kharkiv National Agrarian University named after V. V. Dokuchaev,
educational town of KhNAU, Dokuchaevske settlement,
Kharkiv region, 62483, Ukraine,
e-mail: vasylishynstanislav@gmail.com
ORCID ID: 0000-0001-5023-9878

IMPROVING THE LEVERS OF DIGITALIZATION RISKS MANAGEMENT OF ECONOMIC SECERITY AND FORMATION OF CYBERSECURITY OF THE ACCONUNING SYSTEM

ISSN 2786-4537 (print). Вісник економіки № 1, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2021

Abstract

Introduction. *The XXI century is the era of the information society, which has radically changed the conditions of living and development of the business entities. That is why a separate direction of the economic research is rapidly developing, related to the development of the measures to strengthen the economic security of the enterprise in the digitalized world.*

The purpose of the research *is to assess the state and develop the ways to improve the management levers of digitalization risks of the economic security and the formation of the cyber security of the accounting system of the enterprises.*

Methods. *To achieve the purpose of research, various methods and techniques were used: a systematic approach (development of an adaptive cybersecurity system as a function of the economic security service of the enterprise); analysis and synthesis (determination of digitalization risks and the nature of their impact on accounting and analytical support); monographic (identification of information security components). In order to deeply analyze the views of the professional environment on certain aspects of accounting and analytical support of economic security in the digital world conducted an all-Ukrainian expert survey of accounting staff, scientists and graduates «The place of economic security in accounting and analytical management and transformation of the accounting profession in the digital world", which lasted during 2019–2020 and covered 858 respondents, of which 62.1% are accountants-practitioners of leading enterprises in Eastern Ukraine. In the process of expert survey, a method of questionnaires of a unique sample of respondents was developed. Since the sample population in one proportion or another necessarily included representatives of all groups, the typification of the general population allowed to exclude the influence of intergroup variance on the average error of the sample, which in this case is determined only by intra-group variation.*

Results. *The structure and types of major infringements in the field of the cyber security of the Ukrainian enterprises have been analyzed. Based on the results of the all-Ukrainian expert questioning of the accountants, the importance of the individual groups and the structure of digitalization risks of accounting and analytical support have been determined. The technical, software, information, personnel and organizational components of the information security of the enterprises have been substantiated. An adaptive cyber security system has been developed as a function of the enterprise's economic security service based on the separation of an expert group on the information security, which is a part of the economic security service and performs the functions of monitoring cyber threats, coordinating tactical actions and forming cyber security strategies or involving IT companies' integrators. Based on the modeling of the measures to respond to and eliminate cyber threats to the information security at different stages of cyber-attacks, the implementation of preventive, reactionary, protective, prognostic and monitoring stages of cyber defense has been proposed.*

Perspectives. *The potential success of the enterprise in the conditions of transformational changes in the economy in the process of digitalization will directly depend on the change of the accounting paradigm, which is a key element of business process modifications and the main source of the information needs of all stakeholder groups related to the economic security.*

Keywords: *digitalization, economic security, cyber security, digitalization risks, accounting system, enterprise.*

Formulas: 0, fig.: 5, table: 2, bibl.: 12.

Актуальність теми. Сучасна економіка України перебуває в процесі адаптації до глобалізаційних змін світового простору, які безпосередньо формують зовнішнє середовище функціонування підприємницьких структур. Водночас, трансформація обліку є об'єктивним явищем у результаті посилення процесів цифровізації світової економіки та запровадження в облікову практику діджитал-технологій (діджиталізації).

Діджиталізація економіки сприяла появі новітніх інтегрованих систем обробки та зберігання фінансової інформації, тому на зміну традиційним формам обліку прийшла автоматизована, яка базується на використанні комплексу програмного забезпечення, що автоматизує до 90 % усіх ручних операцій бухгалтера.

Відповідно до розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації» визначено, що основною метою цифровізації є трансформація наявних і створених у майбутньому нових галузей економіки, а також трансформація сфер життєдіяльності в нові, ефективніші та сучасніші. В Концепції зазначено, що досягнення визначеної мети можливе лише за умови, коли ідеї, дії, ініціативи та програми, які стосуються цифровізації, буде інтегровано в стратегії та програми розвитку на національному, регіональному і галузевому рівнях [1].

Саме тому особливої актуальності набувають питання, пов'язані з розробкою механізмів управління діджиталізаційними ризиками та формуванням кібербезпеки у системі обліково-аналітичного забезпечення економічної безпеки підприємств.

Аналіз останніх досліджень і публікацій. Вплив цифрових технологій на обліково-аналітичне забезпечення та економічну безпеку підприємств розглянуто в працях багатьох науковців, серед яких О. Адамик, Т. Бочуля, В. Дерій, В. Жук, Б. Засадний, А. Крутова, В. Муравський, Л. Соколенко, Д. Тепскот, В. Яценко та ін.

Як влучно зазначили В. Дерій та М. Гуменна-Дерій, «майбутній розвиток людства нині важко собі уявити без повсюдного використання і удосконалення інформаційно-комп'ютерних технологій, що базуються на широкому застосуванні комп'ютерної техніки, мережевих комунікацій, штучного інтелекту тощо. В системах управління бізнесом також постійно відбуватимуться значні зміни, що будуть пов'язані з новими величезними технічними, технологічними та операційними можливостями забезпечення бізнес-процесів, зменшенням витрат на них, збільшенням частки інтелектуальної праці, зменшенням кількості управлінців, посиленням громадського контролю за економічною діяльністю і т. д.» [2, с. 12].

На думку професора Т. Бочулі, як і раніше, найбільшу цінність серед інформаційних ресурсів займає інформація, підготовлена обліковою системою. Можна багато говорити про її ретроспективний характер, проте саме облікові дані є основою подальшого аналізу фінансово-господарського стану підприємства [3, с. 35]. Нині стрімко розвивається окремий напрямок економічних досліджень, пов'язаний з розробкою заходів щодо удосконалення обліку в цифровому світі.

ISSN 2786-4537 (print). Вісник економіки № 1, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2021

Уперше новаторський термін «цифрова економіка» (англ. digital economy) у бізнес-середовище в 1995 р. увів відомий канадський консультант із бізнес-стратегій Дон Тапскотт. За його визначенням, цифрова економіка – це економічна діяльність, яка ґрунтується на застосуванні цифрових технологій. У доступній формі він пояснив, як організації, що орієнтуються на досягнення результатів, проходять шлях від звичайного реінжинірингу до повної трансформації корпорації за допомогою інформаційних технологій [4].

Проте цифровізація всіх сфер суспільного життя, на думку окремих науковців, «не є недосяжною або ілюзорною, це правильний крок на шляху до розвитку глобалізованого суспільства. Цифровізація економіки стає одночасно і середовищем, і інструментом перебігу економічних процесів, забезпечуючи трансформацію складних систем відносин суспільного відтворення» [5, с. 47].

На думку В. Жука, «потенційні можливості виконання бухгалтерським обліком важливої ролі соціально-економічного інституту сьогодні багато в чому зростають на основі використання комп'ютерних технологій, інтернету, інших технологій, які підтримують і розширюють можливості специфічних методів обліку» [6, с. 204]. Саме тому неодмінною складовою побудови безпекоорієнтованої облікової політики та безпекового подання бізнесу у звітності має стати побудова стрункої й ефективної системи управління діджиталізаційними ризиками і загрозами інформаційної безпеки (кібербезпеки) підприємств.

Наукові праці вчених становлять потужну теоретичну та практичну базу, що свідчить про велику актуальність досліджуваного питання, але напрямки формування кібербезпеки як складової економічної безпеки підприємств в умовах посилення кіберризиків у цифровому світі вивчено недостатньо глибоко, що зумовлює необхідність подальших досліджень.

Мета дослідження. Метою дослідження є оцінювання стану та розробка шляхів удосконалення важелів управління діджиталізаційними ризиками економічної безпеки і формування кібербезпеки облікової системи підприємств.

Виклад основного матеріалу. Сучасна наукова дисципліна оперує декількома категоріями, які відображають процес всеохопного проникнення цифрових технологій у всі сфери суспільного життя (поняття «цифровізація», «діджиталізація», «інформатизація», «комп'ютеризація» тощо). З погляду зміцнення економічної безпеки, уважаємо за доцільне застосовувати категорію «діджиталізація» (від англ. digitalization – оцифровування, переведення інформації в цифрову форму). Цей термін ми ототожнюємо з явищем цифровізації, яка не має єдиної інтерпретації у зв'язку зі своєю багатогранністю та глобальністю безперечного впливу на усі сфери життя суспільства.

Потенційний успіх підприємства в умовах трансформаційних змін економіки в процесі діджиталізації прямо залежатиме від зміни бухгалтерської парадигми, яка є основним елементом модифікацій щодо бізнес-процесів, і провідним джерелом задоволення інформаційних потреб усіх груп стейкхолдерів, пов'язаних з економічною безпекою підприємницьких структур. Тому провідні дослідники одним з визначальних напрямків у зміцненні економічної безпеки вважають інформаційну складову, яка охоплює нагромаджений масив інформації бухгалтерського обліку.

Інформаційна безпека – це оптимальний стан стабільності і захищеності інформаційної оболонки підприємства, який унеможливлює її втрату, несанкціоноване розповсюдження та забезпечує її захист в інтересах власників підприємства чи держави.

Наголосимо, що Україна через недосконалість національного законодавства та високий рівень кіберзлочинного напруження є країною з високим ризиком діджиталізованих загроз у стратегічно важливих галузях національної економіки, зокрема в аграрному секторі. 27 червня 2017 р. всесвітньо відомий вірус WannaCry, який в Україні отримав назву Petya A, або «Петя» атакував інформаційні оболонки провідних українських компаній, серед яких стратегічно важливі: «Київенерго», «Укртелеком», «Ощадбанк», «Нова пошта», «Укрпошта», «Приватбанк», «Укрзалізниця», аеропорт «Бориспіль», Укренерго, мережа заправок ТНК, «Антонов», Київводоканал, ДТЕК, Київський метрополітен, Кіберполіція, Нацполіція, Міністерство внутрішніх справ, Міністерство культури тощо. Найбільших збитків було завдано саме інформаційним базам даних, особливо інформації про клієнтів та внутрішнім інформаційним потокам цих компаній. Колосальні втрати від вірусу досі важко оцінити (рис. 1).

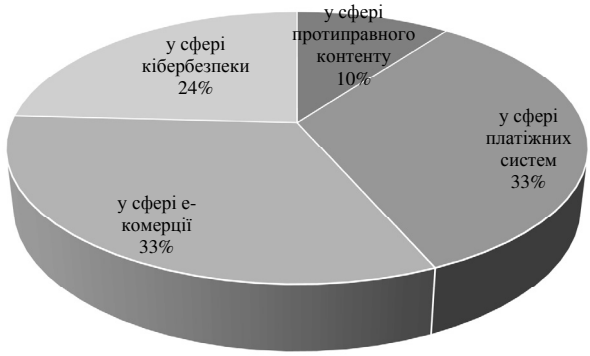

Рис. 1. Структура і типи кримінальних проваджень, порушених Департаментом кіберполіції Національної поліції України у 2018 р.
Джерело: побудовано за [7].

Незважаючи на зростання суспільного резонансу та розкриття масштабних кібератак, бізнес і сьогодні недостатньо фінансує кібербезпеку, що призводить до мільярдних збитків. Крім того, якщо великим компаніям завдають великих збитків кібератаки у вигляді наведених вище витрат, то для середніх і малих компаній вони можуть становити загрозу їхньому існуванню. Величезна шкода через відсутність стратегії розвитку підприємств у разі кібератак актуалізує необхідність пошуку новітніх методів захисту інформаційної оболонки як системоутворювального принципу обліково-аналітичного забезпечення управління економічною безпекою.

Як зазначає В. Ф. Яценко, науково-технічний процес спричиняє трансформаційні зміни системи бухгалтерського обліку у зв'язку із поширенням інформаційних технологій та систем, автоматизованих мереж, масового оцифрування інформації тощо [8, с. 76]. Ми повністю погоджуємось з цією думкою і вважаємо, що процеси діджиталізації, поява хмарних технологій зберігання баз даних, віртуальних офісів,

ISSN 2786-4537 (print). Вісник економіки № 1, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2021

ботів, штучного інтелекту, бізнес-сайтів тощо вимагає повної перебудови системи бухгалтерського обліку з метою оптимізації управлінської функції.

Результати експертного опитування 533 бухгалтерів-практиків свідчать, що 33 % діджиталізаційних ризиків підприємств пов'язані з фізичним виходом техніки з ладу, 27 % – з розкриттям комерційної таємниці, 20 % – з несанкціонованим витоком інформації внаслідок кібератак (рис. 2).

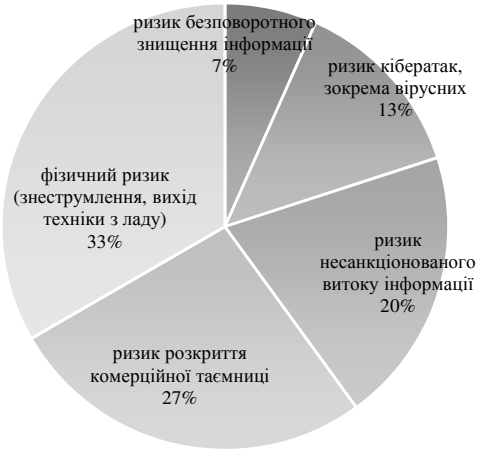

Рис. 2. Вагомість окремих груп діджиталізаційних ризиків обліково-аналітичного забезпечення.
Джерело: побудовано за результатами всеукраїнського експертного опитування.

Під комп'ютерною системою бухгалтерського обліку О. В. Адамик розуміє «взаємопов'язану сукупність інформації про господарські операції, програмних засобів та специфічних алгоритмів її обробки, що реалізовані з допомогою комплексу обчислювальних, комунікаційних й інших технічних засобів, та фахівців-бухгалтерів з метою надання інформації нової якості для ухвалення ефективних управлінських рішень» [9, с. 168]. Основним позитивним результатом суцільної автоматизації обліку є те, що час, який бухгалтери витрачають на обробку документів та формування звітів, значно скоротився і, відповідно, може бути використаний на удосконалення наявної в підприємстві системи класифікації інформаційних ресурсів та на творче узагальнення й аналіз інформації, отриманої на різних етапах облікової обробки [10].

Автоматизація обліку – це шлях до мінімізації впливу людського чинника на реалізацію облікових функцій та ухвалення управлінських рішень. Людський чинник пов'язаний з високою ймовірністю формування навмисного викривлення висновків, облікової інформації, появою випадкових технічних помилок, отриманням особистої вигоди чи збагаченням шляхом здійснення махінацій з активами і зобов'язаннями підприємства [11]. В результаті автоматизації виникла необхідність формування технічного, програмного, інформаційного, кадрового та організаційного компонентів інформаційної безпеки (табл. 1).

Таблиця 1

Компоненти інформаційної безпеки підприємств

Назва компонента	Характеристика
Технічний	Комплекс комп'ютерної техніки: процесори, монітори, модеми, кабелі, принтери, інші канали зв'язку
Програмний	Сукупність програмного забезпечення і його модулів; операційні системи та їх налаштування
Інформаційний	Сукупність облікової інформації, яка зберігається в електронному вигляді, на носіях внутрішньої і зовнішньої пам'яті
Кадровий	Персонал бухгалтерської служб та підрозділів, які мають доступ до бухгалтерської інформації й її захисту
Організаційний	Підрозділ чи працівник, який відповідає за зберігання комерційної таємниці і захист облікової інформації

Джерело: авторська розробка.

За визначенням Б. А. Засадного, інформаційні ризики – це ризики, які виникають під впливом розповсюдження спаму, комп'ютерних вірусів, махінацій із фінансовою звітністю, навмисне викривлення інформації про діяльність підприємства в Інтернеті, несанкціонований доступ сторонніх осіб до комерційної таємниці тощо [12, с. 112].

Серед найбільш поширених у бухгалтерській практиці діджиталізаційних ризиків, які часто призводять до порушення інформаційної оболонки підприємства, експерти називають вірусні атаки внутрішньої комп'ютерної мережі (27 %), відкриття вірусних файлів, які надійшли на електронну пошту (24 %), збій електропостачання та фізичне пошкодження носіїв інформації (20 %) (рис. 3). Крім електронної пошти, уразливими до діджиталізаційних ризиків залишаються програми автоматизації бухгалтерського обліку. Майже 39 % опитаних експертів вважають, що найбільш вразлива до кібератак програми – MEDoc, 26,9 % – Клієнт-банк, 23,1 % – 1С: Бухгалтерія. Водночас, на думку експертів, найбільш надійними програмами є SAP ERP, SAP S4/HANA, SAP Business One, УПП та BAS ERP. Ця ситуація свідчить про важливість постійного навчання персоналу бухгалтерських служб основам кіберзахисту, використання складних і надійних інструментів захисту корпоративних електронних пошт підприємств.

Отже, кібербезпека є вагомою складовою загальної економічної безпеки, оскільки вона спрямована на захист бухгалтерської інформації підприємства від загроз, а отже, від негативних економічних наслідків. Водночас, під час розгляду діджиталізаційних ризиків важливо встановити стадії їхнього впливу на інформаційну оболонку, тому пропонуємо розглядати їх як кіберзагрози, кіберінциденти та кібератаки. Як кіберзагрози можна розглядати можливі (з певним ступенем імовірності) несприятливі події, які можуть завдати шкоди інформаційній безпеці підприємства. Кіберінцидент – це подія, що вже відбулася, але піддається оперативному вирішенню. Найбільш деструктивною є кібератака, наслідком якої може бути втрата глобальних баз даних і безповоротне знищення (втрата) інформації, що може призвести до призупинення бізнес-діяльності. Наголосимо, що заходи із попередження та подолання наслідків кіберінцидентів, а особливо – кібератак, повинні відбуватися лише у правовому полі з відповідним залученням правоохоронних органів, зокрема Департаменту кіберполіції Національної поліції України.

ISSN 2786-4537 (print). Вісник економіки № 1, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2021

Рис. 3. Структура діджиталізаційних ризиків, що з ними стикалися в професійній діяльності бухгалтери-практики, які брали участь у всеукраїнському експертному опитуванні

Джерело: побудовано за результатами всеукраїнського експертного опитування.

Вважаємо, що захист облікової інформації має бути компетенцією експертної групи з інформаційної безпеки, яка є складовою служби економічної безпеки і виконує функції моніторингу кіберзагроз, координації тактичних дій та формування стратегій кіберзахисту підприємств (рис. 4). В умовах обмеженості фінансових ресурсів малих і середніх аграрних підприємств доцільно залучити послуги IT-компаній інтеграторів, основне завдання яких – формування кіберзахисту інформаційних оболонок бізнесу.

Основними етапами в процесі організації захисту облікової інформації є такі:

1) ідентифікація загроз інформаційній безпеці;

2) установлення та контроль ризиків і особливостей інформаційного забезпечення управління ними;

3) побудова моделі управління ризиками та його інформаційного забезпечення;

4) формування системи заходів щодо протидії загрозам інформаційній безпеці;

5) розробка організаційних регламентів захисту облікової інформації;

6) контроль інформаційної безпеки та оцінювання заходів її забезпечення.

Як правило, усі здійснювані кіберзлочини мають єдину послідовність дій кіберзлочинців, що зумовлює необхідність поетапного управління ризиками діджиталізації (рис. 5).

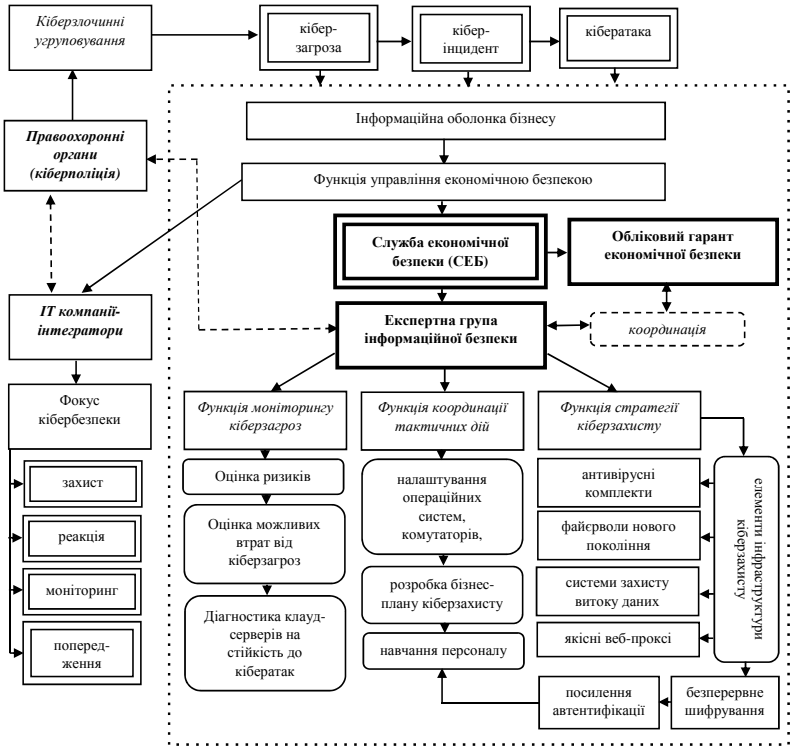

Рис. 4. Адаптивна система забезпечення кібербезпеки як функції служби економічної безпеки підприємства

Джерело: розроблено автором.

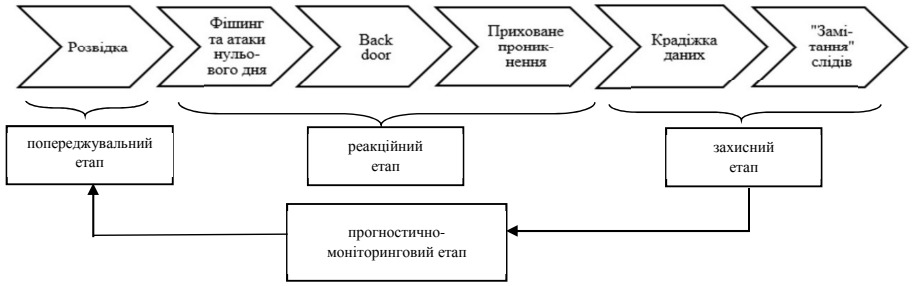

Рис. 5. Модель реагування і нівелювання кіберзагроз інформаційної безпеки на різних стадіях кібератак.

Джерело: розроблено автором.

Зокрема, метою попереджувального етапу є оцінка (розвідка) можливого впливу кіберризиків. На етапах фактичного проникнення кіберзлочинців у середину інформаційної оболонки необхідним є реакційний етап негайного блокування кіберінциденту (чи кібератаки), а на захисному етапі – максимально можливе збереження доступного обсягу інформації та її перенесення на інші носії чи хмарні сховища. Мета прогностично-моніторингового етапу – постійне відстежування вже

ISSN 2786-4537 (print). Вісник економіки № 1, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2021

відомих і потенційних діджиталізаційних ризиків та прогнозування сценаріїв їхнього впливу на інформаційну і, як наслідок, економічну безпеку підприємств.

У результаті попереджувального, реакційного, захисного та прогностично-моніторингового етапу кіберзахисту можливе поступальне планування і реалізація відновлювальних заходів унаслідок впливу кібератак на економічну безпеку в коротко-, середньо- та довгостроковій перспективі (табл. 2).

Отже, повна автоматизація сучасної мережі бухгалтерського обліку, застосування хмарних технологій зберігання інформації дасть змогу побудувати надійні інформаційні зв'язки в середині бухгалтерської служби і між бухгалтерією та іншими структурними підрозділами підприємства. Проте, це можливо лише за умови розробки ефективних стратегій формування кібербезпеки облікового простору, навчання персоналу і збільшення витрат на кіберзахист підприємств.

Таблиця 2

Відновлювальні заходи внаслідок впливу кібератак на економічну безпеку

Рівень реагування	Період реагування	Заходи
Короткостроковий (оперативний)	Дні/тижні	Пошук компромісів захисту від кібератак
		Діагностика заходів кіберзахисту і їх організаційного забезпечення
		Комунікативна взаємодія з контрагентами
		Забезпечення безперервності бізнес-процесів
Середньостроковий (перманентний)	Тижні/місяці	Побудова інфраструктури кіберзахисту й архітектури кібер-менеджменту
		Перманентна взаємодія з адвокатськими та судовими інституціями сфери кіберзахисту
		Моніторинг та оцінювання ймовірних економічних небезпек на основі оцінки попередніх і потенційних кіберзагроз
Довгостроковий (стратегічний)	Місяці/роки	Збільшення інвестицій у розробку або придбання кіберпрограм інформаційної безпеки
		Відновлення бізнесу, який зазнав шкоди внаслідок кібератак у попередні періоди
		Формування банку (архіву) даних кіберзахисту

Джерело: розроблено автором.

Висновки і перспективи подальших досліджень. Досягнення оптимального стану стабільності та захищеності облікових систем підприємств, який унеможливлює втрату інформації, її несанкціоноване розповсюдження і захист в інтересах власників підприємства або держави можливе лише за умови застосування системно-наукового підходу до формування стратегій і тактик кіберзахисту в діджиталізованому світі. Завчасне розроблення заходів протидії діджиталізаційним ризикам є запорукою економічної безпеки та конкурентного розвитку підприємств, успіху розвитку національної економіки.

Єдність дій щодо попередження впливу кіберзагроз, ураховуючи мережі, програмне забезпечення, інформацію та бази даних, персонал, дає змогу досягти синергетичного ефекту заходів з кіберзахисту інформаційної оболонки аграрних підприємств. Необхідної уваги власників та працівників потребує рівень забезпечення безпеки і розроблення необхідних важелів щодо уникнення діджиталізаційних ризиків, зокрема вирішення питання про організацію інформаційної безпеки за рахунок створення окремого підрозділу (експертної групи в межах підрозділу) або залучення професійних ІТ-компаній.

На основі моделювання заходів із реагування та нівелювання кіберзагроз інформаційної безпеки на різних стадіях кібератак запропоновано реалізацію попереджувального, реакційного, захисного і прогностично-моніторингового етапів кіберзахисту. Як наслідок, стає реальним поступальне планування та реалізація відновлювальних заходів після впливу кібератак на економічну безпеку в коротко-, середньо- і довгостроковій перспективі.

Потенційний успіх підприємства в умовах трансформаційних змін економіки у процесі діджиталізації прямо залежатиме від зміни бухгалтерської парадигми, яка є основним елементом модифікацій щодо бізнес-процесів, і головним джерелом задоволення інформаційних потреб усіх груп стейкхолдерів, пов'язаних з економічною безпекою підприємницьких структур.

Література

1. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації : розпорядження Кабінету Міністрів України № 67–р від 17 січня 2018. URL: https://zakon.rada.gov.ua/laws/show/67–2018–%D1%80 (дата звернення 10.03.2020).
2. Дерій В. А., Гуменна-Дерій М. В. Управлінський облік і аналіз бізнес-процесів у підприємстві. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу.* 2018. Вип. 2 (40). С. 12–18.
3. Бочуля Т. В. Облікова складова інформаційного потенціалу підприємства. *Бюл. Міжнар. Нобелів. екон. форуму.* 2013. № 1 (6). С. 35–42.
4. Tapscott D. The Digital Economy. URL: http://dontapscott.com/books/the-digital-economy/ (дата звернення 05.03.2020).
5. Соколенко Л. Ф. Цифровізація як вектор розвитку економічних систем та модернізації системи бухгалтерського обліку. *Облік і фінанси.* 2019. Вип. 85. С. 40–48.
6. Жук В. М. Розвиток теорії бухгалтерського обліку: інституціональний аспект: моногр. Київ : ННЦ «ІАЕ», 2018. 408 с.
7. Офіційний сайт Кіберполіції України. URL: https://cyberpolice.gov.ua/results/2018/ (дата звернення 29.03.2020).
8. Яценко В. Ф. Вплив еволюційної трансформації соціально–економічної системи на теорію бухгалтерського обліку. *Економіка харчової промисловості.* 2019. Вип. 4. С. 71–79.

ISSN 2786-4537 (print). Вісник економіки № 1, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2021

9. Адамик О. В. Розмежування понять «автоматизовані», «комп'ютерні» та «інформаційні» системи бухгалтерського обліку. *Економічний аналіз.* 2016. Т. 26. № 1. С. 163–169.
10. Крутова А. С., Фадєєва Г.М. Методологія та організація ведення обліку в умовах автоматизації. *Облік і фінанси АПК.* 2010. Вип. 4. С. 48–52.
11. Муравський В. В. Понятійно–термінологічний апарат в автоматизації обліку. *Вісник Запорізького національного університету.* 2018. № 2. С. 65–71.
12. Засадний Б. А. Ризики системи бухгалтерського обліку в умовах застосування МСФЗ. *Науковий вісник Ужгородського національного університету.* 2017. Вип. 14. С. 111–115.

References

1. Kabinet Ministriv Ukrajiny. (2018). Pro skhvalennja Koncepciji rozvytku cyfrovoji ekonomiky ta suspiljstva Ukrajiny na 2018–2020 roky ta zatverdzhennja planu zakhodiv shhodo jiji realizaciji [On approval of the Concept of development of the digital economy and society of Ukraine for 2018-2020 and approval of the action plan for its implementation]. Retrieved from: https://zakon.rada.gov.ua/laws/show/67–2018–%D1%80 (accessed 10 March 2020) [Ukrainian].
2. Derij V. A., Ghumenna-Derij M. V. (2018). Upravlinsjkyj oblik i analiz biznes-procesiv u pidpryjemstvi [Management accounting and analysis of business processes in the enterprise]. *Problemy teorii ta metodolohii bukhhalterskoho obliku, kontroliu i analizu – Problems of theory and methodology of accounting, control and analysis,* 2 (40), 12–18 [Ukrainian].
3. Bochulja T. V. (2013). Oblikova skladova informacijnogho potencialu pidpryjemstva [Accounting component of the information potential of the enterprise]. *Biul. Mizhnar. Nobeliv. ekon. forumu – Bulletin of the International Nobel Economic Forum, vol. 1,* no. 6, 35–42 [Ukrainian].
4. Tapscott D. (1994). The Digital Economy. Retrieved from: http://dontapscott.com/books/the-digital-economy (accessed 5 March 2020) [English].
5. Sokolenko L. F. (2019). Cyfrovizacija jak vektor rozvytku ekonomichnykh system ta modernizaciji systemy bukhghaltersjkogho obliku [Digitization as a vector of development of economic systems and modernization of the accounting system]. *Oblik i finansy – Accounting and finance,* 85, 40–48 [Ukrainian].
6. Zhuk V. M. (2018). Rozvytok teoriji bukhghaltersjkogho obliku: instytucionaljnyj aspekt [Development of accounting theory: institutional aspect]. Kyiv: NSC "IAE" [Ukrainian].
7. Kiberpolicija Ukrajiny [Cyberpolice of Ukraine]. Retrieved from: https://zakon.rada.gov.ua/laws/show/67–2018–%D1%80 (accessed 29 March 2020) [Ukrainian].
8. Jacenko V. F. (2019). Vplyv evoljucijnoji transformaciji socialjno–ekonomichnoji systemy na teoriju bukhghaltersjkogho obliku [The influence of the evolutionary transformation of the socio-economic system on the theory of accounting]. *Ekonomika kharchovoi promyslovosti – Economics of the food industry,* 4, 71–79 [Ukrainian].

9. Adamyk O. V. (2016). Rozmezhuvannja ponjatj «avtomatyzovani», «komp'juterni» ta «informacijni» systemy bukhghaltersjkogho obliku [Distinguishing between the concepts of "automated", "computer" and "information" accounting systems]. *Ekonomichnyi analiz – Economic analysis,* vol. 26, no. 1, 163–169 [Ukrainian].
10. Krutova A. S., Fadjejeva Gh. M. (2010). Metodologhija ta orghanizacija vedennja obliku v umovakh avtomatyzaciji [Methodology and organization of accounting in terms of automation]. *Oblik i finansy APK – Accounting and finance of agro-industrial complex,* 4, 48–52 [Ukrainian].
11. Muravsjkyj V. V. (2018). Ponjatijno–terminologhichnyj aparat v avtomatyzaciji obliku [Conceptual and terminological apparatus in accounting automation]. *Visnyk Zaporizkoho natsionalnoho universytetu – Bulletin of Zaporizhia National University,* 2, 65–71 [Ukrainian].
12. Zasadnyj B. A. (2017). Ryzyky systemy bukhghaltersjkogho obliku v umovakh zastosuvannja MSFZ [Risks of the accounting system in terms of application of IFRS]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu – Scientific Bulletin of Uzhhorod National University,* 14, 111–115 [Ukrainian].

Статтю отримано 16 серпня 2020 р.
Article received August 16, 2020

ISSN 2786-4537 (print). Вісник економіки № 1, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2021