УДК 657.1.011.56:004
JEL: M41; O33

КІБЕРБЕЗПЕКА ТА ЗАХИСТ БУХГАЛТЕРСЬКИХ ДАНИХ В УМОВАХ ЗАСТОСУВАННЯ НОВІТНІХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

©2019 **ПОПІВНЯК Ю. М.**

УДК 657.1.011.56:004
JEL: M41; O33

Попівняк Ю. М. Кібербезпека та захист бухгалтерських даних в умовах застосування новітніх інформаційних технологій

Стрімкий розвиток інформаційних технологій та впровадження їх у практику ведення бухгалтерського обліку поставили під загрозу безпеку облікових даних, які циркулюють у кіберсередовищі, та вивели на передній план проблеми визначення заходів щодо підвищення їх кібербезпеки. Мета даної статті – розкриття сучасного стану такої безпеки, а також ідентифікація кіберзагроз у сфері використання бухгалтерської інформації та визначення засобів її захисту від викрадення, пошкодження чи втрати у кіберпросторі. Ґрунтуючись на аналізі статистичних даних, опублікованих у вітчизняних та іноземних дослідженнях, описано стан кібербезпеки у світі за різними показниками, основні джерела кіберзагроз для облікової інформації на підприємстві, а також ситуацію з кіберзлочинністю в Україні. Систематизовано підходи вчених до групування кіберзагроз і сформульовано передумови виникнення цих загроз для бухгалтерської інформації як у цілому, так і при впровадженні окремих, перспективних для використання в бухгалтерському обліку, технологій. Обґрунтовано побудову системи заходів гарантування кібербезпеки бухгалтерської інформації на підприємстві, яка базується на застосуванні загальних і специфічних засобів захисту організаційного, технічного, кадрового та юридичного характеру. Перспективами подальших досліджень у даному напрямі визначено пошук критеріїв та оцінку успішності впровадження заходів із захисту бухгалтерської інформації й гарантування її кібербезпеки.

Ключові слова: *загроза, захист бухгалтерської інформації, інформаційні технології, кібербезпека, кіберзахист.*
DOI: *https://doi.org/10.32983/2222-4459-2019-8-150-157*
Рис.: *3.* ***Бібл.:*** *24.*

Попівняк Юлія Михайлівна *– кандидат економічних наук, доцент кафедри обліку і аудиту, Львівський національний університет імені Івана Франка (вул. Університетська, 1, Львів, 79000, Україна)*
E-mail: *yuliia.popivniak@lnu.edu.ua*
ORCID: *http://orcid.org/0000-0001-7458-0587*
Researcher ID: *http://www.researcherid.com/X-4857-2019*
SPIN: *http://elibrary.ru/3370-2205*

УДК 657.1.011.56:004
JEL: M41; O33

Попивняк Ю. М. Кибербезопасность и защита бухгалтерских данных в условиях применения современных информационных технологий

Стремительное развитие информационных технологий и их внедрение в практику ведения бухгалтерского учета поставили под угрозу безопасность учетных данных, циркулирующих в киберпространстве, и вывели на передний план проблемы определения мероприятий по повышению их кибербезопасности. Цель данной статьи – раскрытие современного состояния такой безопасности, а также идентификация киберугроз в сфере использования бухгалтерской информации и определение средств её защиты от кражи, повреждения или потери в киберпространстве. Основываясь на анализе статистических данных, опубликованных в отечественных и иностранных исследованиях, описаны состояние кибербезопасности в мире по разным показателям, основные источники киберугроз для учетной информации на предприятии, а также ситуация с киберпреступностью в Украине. Систематизированы подходы ученых к группировке киберугроз и сформулированы предпосылки возникновения этих угроз для бухгалтерской информации как в целом, так и при внедрении отдельных, перспективных для использования в бухгалтерском учете, технологий. Обосновано построение системы мер обеспечения кибербезопасности бухгалтерской информации на предприятии, основанной на применении общих и специфических средств защиты организационного, технического, кадрового и юридического характера. Перспективами дальнейших исследований в данном направлении определены поиск критериев и оценка успешности внедрения мероприятий по защите бухгалтерской информации и обеспечения её кибербезопасности.

Ключевые слова: *угроза, защита бухгалтерской информации, информационные технологии, кибербезопасность, киберзащита.*
Рис.: *3.* ***Библ.:*** *24.*

Попивняк Юлия Михайловна *– кандидат экономических наук, доцент кафедры учета и аудита, Львовский национальный университет имени Ивана Франко (ул. Университетская, 1, Львов, 79000, Украина)*
E-mail: *yuliia.popivniak@lnu.edu.ua*
ORCID: *http://orcid.org/0000-0001-7458-0587*
Researcher ID: *http://www.researcherid.com/X-4857-2019*
SPIN: *http://elibrary.ru/3370-2205*

UDC 657.1.011.56:004
JEL: M41; O33

Popivniak Yu. M. Cybersecurity and Protection of Accounting Data under Conditions of Modern Information Technology

The rapid development of information technology and its introduction into accounting practices have jeopardized the security of accounting data circulating in cyberspace and brought to the fore the problems of defining measures to increase their cybersecurity. The article is aimed at disclosing the current status of such security, as well as identifying cyberthreats in the sphere of use of accounting information, and defining the means for its protection against theft, damage or loss in cyberspace. Based on an analysis of statistics published in both domestic and foreign studies, the status of cybersecurity in the world is described according to various indicators, the main sources of cyberthreats for accounting information at enterprise, as well as situation with cybercrime in Ukraine are discussed. The approaches of scholars to grouping the cyberthreats are systematized and the preconditions for the emergence of these threats for accounting information both in general and in the introduction of separate technologies that are promising for use in accounting are formulated. The construction of a system of measures to ensure the cybersecurity of accounting information at enterprise, based on the use of common and specific means of protection of organizational, technical, personnel and legal nature, is substantiated. Prospects for further research in this direction are determined as search for criteria plus assessment of the success of implementation of the measures to protect accounting information and ensure its cybersecurity.

Keywords: *threat, protection of accounting information, information technology, cybersecurity, cyberdefense.*
Fig.: *3.* ***Bibl.:*** *24.*

Popivniak Yuliia M. *– PhD (Economics), Associate Professor of the Department of Accounting and Auditing, Ivan Franko National University of Lviv (1 Universytetska Str., Lviv, 79000, Ukraine)*
E-mail: *yuliia.popivniak@lnu.edu.ua*
ORCID: *http://orcid.org/0000-0001-7458-0587*
Researcher ID: *http://www.researcherid.com/X-4857-2019*
SPIN: *http://elibrary.ru/3370-2205*

Стрімкий розвиток інформаційних технологій, який розпочався наприкінці XX – на початку XXI століть, сприяв їх упровадженню практично в усі сфери людської життєдіяльності та масовому (часто навіть неконтрольованому) використанню, а також формуванню єдиного інформаційного й цифрового простору. При цьому швидкими темпами зросла й кількість зловживань, правопорушень та інших кіберзагроз, спрямованих на різні аспекти діяльності підприємств, які функціонують у кожному з цих просторів.

Інформація про всі факти господарської діяльності підприємства, яка формується в системі його бухгалтерського обліку, характеризується високим ступенем цінності та є запорукою стійкості, розвитку та ефективності діяльності такого підприємства, але лише за умови її надійного захисту. Проте тотальна автоматизація, яка не оминула й сферу бухгалтерського обліку та передбачає впровадження спеціалізованих сучасних технологій і програм для його ведення, попри беззаперечні переваги, ставить під загрозу витоку інформації, хакерських атак, зламу інформаційних мереж, різного роду шахрайства тощо всі облікові дані, які обробляються та зберігаються в цифровому середовищі. На перший план за таких умов виходить забезпечення підприємством особливого виду безпеки інформації – кібербезпеки.

Аналіз останніх досліджень і публікацій. Різні аспекти захисту облікової інформації за умови автоматизованого ведення бухгалтерського обліку розглянуто у працях таких учених, як С. С. Баванет, К. П. Боримська, Ф. Ф. Бутинець, С. А. Вітер, І. Л. Грабчук, Х. Ґров, А. П. Дикий, В. В. Євдокимов, С. В. Івахненков, І. Ю. Кравченко, Г. І. Ляхович, В. В. Муравський, А. С. Марков, Ю. Ю. Мороз, Н. В. Наконечна, В. Ф. Палій, М. С. Пушкар, І. І. Світлишин, В. В. Сторож, В. Л. Цирлов, Н. Л. Шишкова, В. Д. Шквір, В. А. Шпак, Ю. С. Цаль-Цалко та ін.

Однак проблеми кібербезпеки (ідентифікація та групування кібезрагроз, вжиття заходів щодо їх мінімізації чи ліквідації, побудова на підприємстві адекватної системи захисту облікової інформації тощо) на сьогодні досліджені мало. Багато із них, на фоні загострення конкуренції та винайдення щоразу нових інформаційних технологій, залишаються невирішеними та потребують пильного розгляду та уваги науковців, особливо в контексті врахування вітчизняних особливостей ведення бухгалтерського обліку на підприємствах.

Мета статті – розкриття стану кібербезпеки та ідентифікація кіберзагроз у сфері використання облікової інформації, формулювання заходів з мінімізації ризиків викрадення, пошкодження чи втрати даних бухгалтерського обліку в кіберсередовищі його ведення.

Насамперед зазначимо, що поглиблення автоматизації облікових робіт – невідворотне і, загалом, позитивне явище, адже дозволяє значно зекономити ресурси підприємства, підвищити якість обробки інформації, гнучкість, мобільність, інноваційність та ефективність роботи бухгалтера, пришвидшити її цифрову трансформацію, забезпечити доступ до широкого вибору сучасних бухгалтерських програм, хмарних рішень та інших інструментів інформаційних технологій тощо. Одним із негативних моментів застосування комп'ютерних технологій є вразливість облікових даних до кіберзагроз, яку можна мінімізувати за умови застосування правильних способів захисту.

Загалом склад і обсяг бухгалтерських даних, які вважаються комерційною таємницею на підприємстві, а також порядок їх захисту, керівник (власник) цього підприємства визначає самостійно в межах норм чинного законодавства, адже «саме захист комерційної таємниці є найбільш важливим питанням у процесі використання такої інформації» [1, с. 9].

Безпеку визначають як ступінь захисту від злочинної діяльності, небезпеки, пошкодження та/або втрати [2, с. 1175]. Аналізуючи дослідження науковців, поряд з кібербезпекою зустрічаємо термін «інформаційна безпека». Погоджуємося з підходом Р. фон Солмса та Дж. ван Нікерка, які наполягають на різниці між згаданими поняттями. Причому кібербезпека виходить за межі простої інформаційної безпеки та передбачає захищеність різних активів підприємства (не лише інформації), які піддаються ризику при застосуванні таким підприємством комп'ютерних систем і телекомунікаційних мереж [3]. Водночас інформаційна безпека, як процес збереження конфіденційності, цілісності та доступності інформації [4], поряд з електронною інформацією, включає захист інформаційних ресурсів, які опрацьовуються та зберігаються без використання комп'ютерної техніки. У межах нашого дослідження розглядаємо саме кібербезпеку, причому лише у сфері захисту бухгалтерської інформації, яка не просто зберігається на окремому комп'ютері користувача, а циркулює в кіберпросторі – середовищі, що складається з інформаційних систем по всьому світу, включаючи мережі, які поєднують ці системи [5, с. 498; 6].

У процесі опитування працівників, які займаються безпекою інформаційних технологій, проведеного CyberEdge Group, виявлено, що у 2019 р. у середньому 78% кіберзагроз були вдалими (близько 63% усіх підприємств піддалися таким загрозам [7, p. 12]), причому країнами-лідерами в цьому контексті виступили Іспанія (93,7%), Саудівська Аравія (91,5%) та Колумбія (87,9%). Джерелами основної небезпеки нині є шкідливі програми, фішингові атаки, програми-вимагачі, зловживання, пов'язані з обліковими записами користувачів (у т. ч. крадіжка особистих даних), відмовами в обслуговуванні (DoS-/DDoS-атаки), атаки на веб-додатки, спам, ботнети, порушення даних, інсайдерські загрози, фізичні маніпуляції (пошкодження, викрадення, втрата даних), витік інформа-

ції, криптоджекінг (новий вид загроз, який полягає в несанкціонованому використанні чужого комп'ютера для добування криптовалюти), кібершпигунство та ін. [8, р. 7, 9; 10, р. 9], а постачальниками засобів кіберзахисту станом на другий квартал 2018 р. – Cisco, Palo Alto Networks, Fortinet, Check Point [11].

Найбільш захищеними від кіберзагроз на підприємствах є веб-сайти та веб-додатки, сервери (фізичні й віртуальні) та сховища даних, а найменше – ноутбуки та мобільні пристрої [8, р. 9].

Важливим показником захищеності інформації в кіберсередовищі тієї чи іншої країни є індекс глобальної кібербезпеки (англ. – *Global Cybersecurity Index*; який розраховується на основі юридичних, технічних, організаційних індикаторів, а також чинників нарощування потенціалу та кооперації). Україна за цим показником відстає від лідерів і займає лише 54 позицію (*рис. 1*) серед 175 країн, знаходячись приблизно на одному рівні з Узбекистаном, Молдовою, Азербайджаном тощо.

Зауважимо, що для ефективної боротьби з кіберзагрозами, у т. ч. й у сфері захисту даних бухгалтерського обліку на підприємствах, вона має бути одним із пріоритетів державної політики, затверджених на законодавчому рівні. Основними вітчизняними нормативно-правовими актами щодо врегулювання питань, пов'язаних з безпечним функціонуванням учасників кіберпростору, є:

1) Закон України «Про основні засади забезпечення кібербезпеки України» (від 05.10.2017 р. № 2163-VIII);

2) Закон України «Про ратифікацію Конвенції про кіберзлочинність» (від 07.09.2005 р. № 2824-IV);

3) Стратегія кібербезпеки України (рішення Ради національної безпеки і оборони України від 27.01.2016 р.);

4) «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» (рішення Ради національної безпеки і оборони України від 29.12.2016 р.);

5) Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (постанова Кабінету Міністрів України від 19.06.2019 р. № 518).

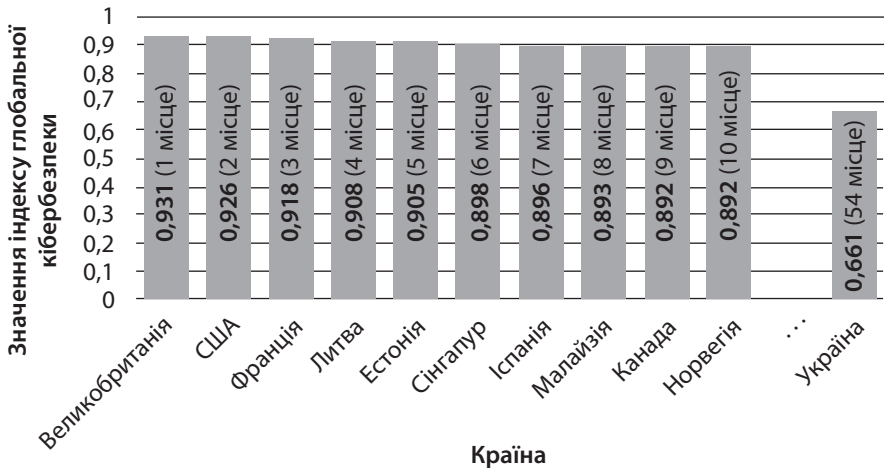

Рис. 1. Місце України в рейтингу країн за показником індексу глобальної кібербезпеки у 2018 р.

Джерело: побудовано автором за даними [12, р. 62–68].

Загалом кількість виявлених і зареєстрованих кіберзлочинів в Україні у 2018 р., порівняно з попереднім роком, дещо знизилася (на 28,7%) [13; 14]. В основному, це відбулося за рахунок покращення ситуації у м. Києві та Київській області. Натомість у таких областях, як Запорізька, Одеська, Миколаївська, кількість злочинів у кіберсфері значно зросла (*рис. 2*). У цілому, трійкою областей з найвищим показником кіберзлочинності в Україні у 2018 р. стали Миколаївська, Одеська і Київська.

За гендерною ознакою 67% вітчизняних кіберзлочинців – чоловіки і, відповідно, 33% кіберзлочинів вчинено жінками. У розрізі видів кіберзлочинів (згідно зі статтями Кримінального кодексу України) їх розподіл виглядає таким чином: 63% – шахрайство, 35% – несанкціоноване втручання в роботу комп'ютерів, 2% – порушення авторського права і суміжних прав [15].

На даний момент українська нормативна база характеризується браком системності, недосконалістю, суперечливістю, розбіжністю підходів, фіскальною спрямованістю, моральною застарілістю та потребує подальшого розвитку й вдосконалення у сфері застосування цифрових технологій та захисту учасників кіберсередовища.

Відповідно до результатів дослідження, отриманих Ernst&Young, середні втрати від порушення цілісності даних у світі у 2017 р. склали 3,62 млн дол. США. При цьому бухгалтерська та фінансова інформація за ступенем привабливості для кіберзлочинців стоїть на другому місці після інформації про клієнтів (12% усіх кіберзагроз) [16, р. 5, 9]. Помилковою є думка, що сказане стосується лише великих і середніх підприємств – кіберзагрозам піддаються дані всіх без винятку суб'єктів господарювання, більше того,

Рис. 2. Темпи зростання зареєстрованих кіберзлочинів в Україні (у розрізі областей) у 2018 р. порівняно з 2017 р.

Джерело: розроблено автором за даними [13; 14].

близько 80% усіх злочинів у цій сфері стосується саме малих підприємств [2, p. 1182].

Зазначимо, що для формування ефективної системи заходів з мінімізації кіберзагроз і адекватного захисту бухгалтерської інформації слід, передусім, визначитися із розумінням поняття «загроза». У дослідженнях М. М. Алані знаходимо таке трактування загрози: «потенційне посягання на безпеку, яке існує за наявності обставин, можливостей, дій або подій, що можуть її порушити і заподіяти шкоду» [17, p. 15–16]. О. А. Євтушевська визначає цей термін як «потенційні або реально можливі дії стосовно інформаційних ресурсів, що призводять до неправомірного оволодіння інформацією» [18, с. 159]. Похідною від загрози є *кіберзагроза*, під якою (розглянувши підходи в економічній літературі та у законодавстві) в контексті нашого дослідження розуміємо *наявну чи потенційну подію, яка несе небезпеку учасникам кіберпростору у сфері функціонування інформаційної системи бухгалтерського обліку, призводить до втрати, пошкодження, знищення чи несанкціонованого використання облікової інформації.*

Обґрунтоване групування кіберзагроз – наступний крок для побудови комплексної системи кібербезпеки облікової інформації на підприємстві. Так, О. А. Євтушевська поділяє загрози на зовнішні, джерелами яких є конкуренти, злочинні групи хакерів і терористичні угруповання, політичні структури тощо, та внутрішні, уособлені адміністрацією і персоналом підприємства [18, с. 159]. Своєю чергою, внутрішні загрози дослідники поділяють на: 1) комп'ютерне шахрайство, комп'ютерну підробку, надання конфіденційної інформації конкурентам [19, с. 232]; 2) технічні загрози, загрози отримання неправдивої інформації, розголошення, інші загрози недосконалої організації [20].

В. А. Нехай та В. В. Нехай слушно доповнюють наведений перелік видом загроз, які пов'язані з навмисними помилками, що виникають за межами бізнесу [21, с. 140]. Джерелом загрози в цьому випадку може виступити, наприклад, бізнес-партнер чи розробник спеціалізованого програмного забезпечення.

Окрім класифікації загроз бухгалтерській інформації за джерелом (місцем, природою) їх виникнення, яка зустрічається у працях науковців найчастіше, вчені виокремлюють ще й такі ознаки групування небезпек: за проявом та наслідками; за типом; за метою; за характером виникнення; за інформаційними технологіями; за об'єктом впливу; за причиною виникнення [21, с. 140]; за часом; за ймовірністю [20].

Паралельно з означенням і класифікацією кіберзагроз, а також ідентифікацією способів, якими може бути порушена безпека даних на підприємстві, важливо також окреслити основні передумови виникнення таких загроз для бухгалтерської інформації:

1) використання неліцензійного або неперевіреного програмного забезпечення для ведення облі-

ку та подання звітності, нехтування його вразливими місцями;

2) застосування слабких інструментів аутентифікації користувачів бухгалтерської інформації;

3) нехтування правилами захисту робочих комп'ютерів чи інших пристроїв, з яких відбуваються доступ і робота з обліковими даними;

4) застосування робочих пристроїв у неробочих цілях;

5) брак у бухгалтерів елементарних знань з основ кібербезпеки;

6) неправильна розстановка пріоритетів і відсутність належної підтримки з боку системи менеджменту підприємства;

7) нехтування правилами збереження бухгалтерських даних і їх періодичного резервування;

8) ігнорування наявних ризиків і негативного досвіду інших учасників ринку;

9) відсутність на підприємстві відповідного спеціаліста із захисту бухгалтерської інформації;

10) довгий перелік осіб, які мають доступ до даних, відсутність розмежування прав користувачів;

11) складне податкове та бізнес-оточення підприємства та ін.

Наслідуючи світові тенденції, бухгалтерський облік все більшої кількості вітчизняних підприємств піддається автоматизації та діджиталізації з використанням таких сучасних інструментів і технологій, як блокчейн, хмарні й туманні технології, штучний інтелект, Інтернет речей, мобільні обчислення, машинне навчання тощо. Кожна зі згаданих технологій, крім загального переліку загроз, наведеного вище, характеризується специфічними ризиками для облікової інформації, які є наслідком сутності та особливостей функціонування тієї чи іншої технології. Наприклад, при використанні мобільних пристроїв для ведення обліку специфічними ризиками будуть: погана обізнаність і культура використання пристроїв, їх втрата і викрадення; нездатність мережевих інженерів швидко ліквідувати вразливості; придбання мобільного пристрою зі заздалегідь встановленим шкідливим програмним забезпеченням (кожен 36-й мобільний пристрій піддається такій загрозі [9, p. 41]); проблеми взаємодії з іншими програмами тощо. Якщо мова йде про Інтернет речей, то тут проблемами стануть ідентифікація підозрілого трафіку, забезпечення відповідності контролю безпеки вимогам сьогодення, оновлення великої кількості підключених до Інтернету речей пристроїв, брак кадрів належної кваліфікації, відстеження доступу до даних та ін.

Хмарні технології ведення бухгалтерського обліку і подання звітності теж не цілком безпечні. Специфічними загрозами для облікової інформації тут можуть стати неможливість використання попередніх версій програмного забезпечення, висока залежність від якості надання послуг провайдерами, непевність стосовно приватності та права власності на дані у хмарі (брак відповідного законодавчого захисту прав на інформацію у хмарному середовищі), складнощі ідентифікації джерела загроз тощо.

Говорячи про технологію блокчейн, якій пророкують велике майбутнє в бухгалтерському обліку й аудиті, специфічними загрозами для інформації, зумовленими особливостями цієї технології, є низький рівень приватності та конфіденційності даних про діяльність підприємства, відсутність законодавчо затвердженої відповідальної особи за ведення розподіленої бази даних про операції, перевантаження пристроїв зберігання інформацією як наслідок невідворотного зростання її обсягів тощо.

Світовий досвід свідчить, що найбільшими проблемами використання ефективних засобів боротьби з кіберзагрозами сьогодні є складнощі їх впровадження й інтеграції, брак відповідних фахівців (низький рівень усвідомлення ними проблем кібербезпеки), фінансових ресурсів, ефективних рішень на ринку, підтримки з боку системи менеджменту підприємства, постійне вдосконалення способів виконання зловмисних дій тощо [8, p. 11, 16]. До перелічених додамо ще обмеження, характерні для вітчизняного середовища господарювання: недосконаліть законодавства у сфері кібербезпеки, політичні ризики, корупція та протекціонізм. Зазначимо, що найбільше коштів на кібербезпеку сьогодні виділяють компанії Мексики (15,9% від IT-бюджету), Бразилії (15,9%) і Південної Африки (14,9%) [8, p. 20].

Л. Колобов та І. Колеснікова поділяють заходи із захисту конфіденційної інформації на юридичні, фізичні, технічні та психологічні [1, с. 11], О. А. Євтушевська – на фізичні, апаратні, програмні й криптографічні [18, с. 160], А. П. Дикий виділяє організаційно-технічні, організаційно-режимні заходи з організації захисту та безпеки облікових даних і кадрову роботу [22, с. 211]. Схожого до останнього підходу дотримуються С. А. Вітер та І. І. Світлишин, які виокремлюють організаційні заходи, технічні заходи та кадрову роботу. На думку цих авторів, система перелічених заходів має відповідати критеріям підтримки програмного забезпечення, охорони конфіденційності інформації, персональної відповідальності, секретності, комплексності, ефективного контролю доступу до облікових даних [5, с. 500–501].

В. А. Шпак до елементів захисту облікової інформації відносить правові, технічні, програмні та організаційні. При цьому «співвідношення елементів та їх зміст забезпечують індивідуальність системи захисту інформації підприємства та гарантують її надійність» [23, с. 182]. Дещо інший погляд – у І. Л. Грабчук, яка серед засобів захисту облікової інформації в електронному вигляді виокремлює засоби логічної та фізичної безпеки [24, с. 23].

Система кіберзахисту бухгалтерської інформації – це комплекс заходів на державному рівні й на рівні окремого підприємства, покликаних гарантувати безпеку та захист такої інформації, як і автоматизованої системи ведення бухгалтерського обліку на підприємстві в цілому, від кіберзагроз. Наведемо сукупність таких засобів захисту на підприємстві в розрізі їх видів на *рис. 3*.

Як бачимо з рис. 3, за аналогією зі загальними та специфічними загрозами, виокремлюємо засоби захисту від них загального та специфічного характеру. При цьому всю їх множину поділяємо на організаційні, технічні, кадрові й юридичні заходи. Ключове значення тут має наявність коштів для реалізації згаданих заходів – чим більший бюджет, тим вищі шанси мінімізувати кіберризики (за умови вдалого використання фінансових ресурсів).

Насамкінець зазначимо, що однією із основних складностей при боротьбі з кіберзагрозами є те, що, за даними Telstra, 78% компаній сьогодні не мають чіткого плану реагування на можливі небезпеки [7, p. 9]. Для захисту від кіберзагроз підприємства найчастіше використовують мережеві антивіруси (63,9%), контроль доступу до мережі (59,8%), SSL/TLS пристрої (платформи) для дешифрування (59,4%) та системи виявлення (запобігання) вторгнень [8, p. 24]. Як варіант розглядається також передача окремих функцій захисту інформації (тестування проникнень, аналіз загроз, моніторинг мережевої безпеки в режимі реального часу та ін.) на аутсорсинг.

ВИСНОВКИ

У сучасному світі розвинутих технологій впровадженням останніх у процес ведення бухгалтерського обліку вже нікого не здивуєш. При цьому бухгалтерська інформація, яка формується у такому процесі, – особливий ресурс, що потребує ретельного захисту, адже від безпечного її використання залежить інформаційна безпека всього підприємства.

Результати проведеного дослідження свідчать, що нині у світі кіберберзагрозам піддається значна частина підприємств, причому незалежно від їх розміру та виду діяльності. Останніми роками в Україні також почастішали кібератаки, які, серед іншого, зумовлені національними особливостями господарювання, такими як брак належної законодавчої бази, велика питома вага підприємств, що використовують неліцензійні бухгалтерські програмні продукти, нехтування правилами захисту автоматизованих робочих місць, брак у спеціалістів з бухгалтерського обліку знань з основ кібербезпеки тощо. Для мінімізації негативного впливу кіберзагроз пропонується комплексна система загальних і специфічних заходів організаційного, технічного, кадрового та юридичного характеру. При цьому критерії оцінки успішності впровадження цих заходів – напрям наших подальших досліджень. ■

ЛІТЕРАТУРА

1. Колобов Л., Колеснікова І. Комерційна таємниця та питання захисту комерційної таємниці. *Цивільне право і процес*. 2016. № 5. С. 8–13.

2. Bawaneh S. S. Information security for organizations and accounting information systems. A Jordan banking sector case. *International Review of Management and Business Research*. 2014. Vol. 3. Issue 2. P. 1174–1188.

3. Von Solms R., van Niekerk J. From information security to cyber security. *Computers & Security*. 2013. Vol. 38. P. 97–102 URL: https://www.sciencedirect.com/science/article/pii/S0167404813000801?via%3Dihub

4. ISO/IEC 27001:2013. Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности. Требования / пер. с англ. А. Горбунов. URL: https://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf

5. Вітер С. А., Світлишин І. І. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство*. 2017. Вип. 11. С. 497–502.

6. National cyber security strategy and 2013–2014 action plan / Ministry of Transport, Maritime Affairs and Communications; Republic of Turkey. URL: https://sherloc.unodc.org/res/cld/lessons-learned/national_cyber_security_strategy_and_2013-2014_action_plan_html/National_Cyber_Security_Strategy_and_2013-2014_Action_Plan.pdf

7. Summary Report / Telstra Security Report 2019. Paddington : Telstra Corporation Limited, 2019. 19 p.

8. 2019 Cyberthreat Defense Report / CyberEdge Group. Annapolis: CyberEdge Group, 2019. 50 p.

9. Internet Security Threat Report / Symantec. Mountain View: Symantec Corporation, 2019. 61 p.

10. 15 Top Cyberthreats and Trends / ENISA Threat Landscape Report 2018. Heraklion: European Union Agency For Network and Information Security, 2018. 138 p.

11. Feldman S. No clear leader in cybersecurity market. URL: https://www.statista.com/chart/16651/cybersecurity-global-market/

12. Global Cybersecurity Index (GCI) 2018 / International Telecommunication Union. Geneva : ITUPublications, 2019. 86 p.

13. Відомості про зареєстровані упродовж січня – грудня 2018 року злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) та результати їх розслідування / Генеральна прокуратура України. URL: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v_4

14. Відомості про зареєстровані упродовж 2017 року злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) та результати їх розслідування / Генеральна прокуратура України. URL: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v_3

15. Підсумки 2018 року в цифрах / Департамент Кіберполіції Національної поліції України. URL: https://cyberpolice.gov.ua/results/2018/

16. Is cybersecurity about more than protection? / EY Global Information Security Survey 2018–19. London : EYGM Limited, 2018. 35 p.

17. Alani M. M. Elements of Cloud Computing Security. A Survey of Key Practicalities. Switzerland : Springer, 2016. 55 p.

18. Євтушевська О. А. Інформаційна безпека як елемент підвищення ефективності комплексного контролю підприємств водного транспорту. *Зовнішня торгівля: економіка, фінанси, право*. 2015. № 5-6. С. 157–162.

Рис. 3. Комплексна система заходів гарантування кібербезпеки бухгалтерської інформації на підприємстві

Джерело: авторська розробка.

19. Муравський В. Забезпечення інформаційної безпеки в автоматизованих системах бухгалтерського обліку. *Економічний аналіз*. 2013. Вип. 12. Ч. 4. С. 232–235.

20. Рожелюк В. М. Заходи забезпечення захисту облікової інформації. Київ: ПП «Рута», 2013 URL: http://dspace.tneu.edu.ua/bitstream/316497/19062/1/Заходи%20забезпечення%20захисту%20облікової%20інформації.pdf

21. Нехай В. А., Нехай В. В. Інформаційна безпека як складова економічної безпеки підприємств. *Науковий вісник Міжнародного гуманітарного університету. Серія «Економіка і менеджмент»*. 2017. Вип. 24 (2). С. 137–140.

22. Дикий А. П. Порядок забезпечення безпеки бухгалтерської інформації в умовах застосування сучасних комп'ютерних технологій. *Проблеми теорії та методоло-*

гії бухгалтерського обліку, контролю і аналізу. 2008. № 3. С. 208–214.

23. Шпак В. А. Організація захисту облікової інформації. *Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації.* 2015. № 2. С. 181–187.

24. Грабчук І. Л. Організація захисту облікової інформації в умовах гібридної війни. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу*. 2018. Вип. 3. С. 20–24.

REFERENCES

Alani, M. M. *Elements of Cloud Computing Security. A Survey of Key Practicalities*. Switzerland: Springer, 2016.

Bawaneh, S. S. "Information security for organizations and accounting information systems. A Jordan banking sector case". *International Review of Management and Business Research*, vol. 3, no. 2 (2014): 1174-1188.

"2019 Cyberthreat Defense Report". In *CyberEdge Group. Annapolis: CyberEdge Group*, 2019.

Dykyi, A. P. "Poriadok zabezpechennia bezpeky bukhhalterskoi informatsii v umovakh zastosuvannia suchasnykh kompiuternykh tekhnolohii" [Procedure for ensuring the security of accounting information in the conditions of application of modern computer technologies]. *Problemy teorii ta metodolohii bukhhalterskoho obliku, kontroliu i analizu*, no. 3 (2008): 208-214.

Feldman, S. "No clear leader in cybersecurity market". https://www.statista.com/chart/16651/cybersecurity-global-market/

"Global Cybersecurity Index (GCI) 2018". In *International Telecommunication Union*. Geneva: ITUPublications, 2019.

Hrabchuk, I. L. "Orhanizatsiia zakhystu oblikovoi informatsii v umovakh hibrydnoi viiny" [Organization of protection of accounting information in the conditions of hybrid war]. *Problemy teorii ta metodolohii bukhhalterskoho obliku, kontroliu i analizu*, no. 3 (2018): 20-24.

"Internet Security Threat Report". In *Symantec. Mountain View: Symantec Corporation*, 2019.

"Is cybersecurity about more than protection?" In *EY Global Information Security Survey 2018-19*. London: EYGM Limited, 2018.

"ISO/IEC 27001:2013. Informatsionnyye tekhnologii. Metody zashchity. Sistemy menedzhmenta informatsionnoy bezopasnosti. Trebovaniya" [ISO / IEC 27001: 2013. Information Technology. Methods of protection. Information Security Management Systems. Requirements]. https://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf

Kolobov, L., and Kolesnikova, I. "Komertsiina taiemnytsia ta pytannia zakhystu komertsiinoi taiemnytsi" [Trade secrets and trade secrets]. *Tsyvilne pravo i protses*, no. 5 (2016): 8-13.

Muravskyi, V. "Zabezpechennia informatsiinoi bezpeky v avtomatyzovanykh systemakh bukhhalterskoho obliku" [Providing information security in automated accounting systems]. *Ekonomichnyi analiz,* vol. 4, no. 12 (2013): 232-235.

"National cyber security strategy and 2013-2014 action plan / Ministry of Transport, Maritime Affairs and Communications; Republic of Turkey". https://sherloc.unodc.org/res/cld/lessons-learned/national_cyber_security_strategy_and_2013-2014_action_plan_html/National_Cyber_Security_Strategy_and_2013-2014_Action_Plan.pdf

Nekhai, V. A., and Nekhai, V. V. "Informatsiina bezpeka yak skladova ekonomichnoi bezpeky pidpryiemstv" [Information security as a component of economic security of enterprises]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriia «Ekonomika i menedzhment»,* no. 24 (2) (2017): 137-140.

"Pidsumky 2018 roku v tsyfrakh" [2018 results in numbers]. Departament Kiberpolitsii Natsionalnoi politsii Ukrainy. https://cyberpolice.gov.ua/results/2018/

Rozheliuk, V. M. "Zakhody zabezpechennia zakhystu oblikovoi informatsii" [Security measures for accounting information]. http://dspace.tneu.edu.ua/bitstream/316497/19062/1/Заходи%20забезпечення%20захисту%20облікової%20інформації.pdf

"15 Top Cyberthreats and Trends". In *ENISA Threat Landscape Report 2018. Heraklion: European Union Agency For Network and Information Security,* 2018.

"Summary Report". In *Telstra Security Report 2019*. Paddington: Telstra Corporation Limited, 2019.

Shpak, V. A. "Orhanizatsiia zakhystu oblikovoi informatsii" [Organization of protection of accounting information]. *Bukhhalterskyi oblik, analiz ta audyt: problemy teorii, metodolohii, orhanizatsii,* no. 2 (2015): 181-187.

"Vidomosti pro zareiestrovani uprodovzh 2017 roku zlochyny u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv) ta rezultaty yikh rozsliduvannia" [Information on crimes recorded in 2017 concerning the use of electronic computers (computers) and the results of their investigation]. Heneralna prokuratura Ukrainy. https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v_3

"Vidomosti pro zareiestrovani uprodovzh sichnia - hrudnia 2018 roku zlochyny u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv) ta rezultaty yikh rozsliduvannia" [Information on crimes recorded in the period from January to December 2018 concerning the use of electronic computers (computers) and the results of their investigation]. Heneralna prokuratura Ukrainy. https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v_4

Viter, S. A., and Svitlyshyn, I. I. "Zakhyst oblikovoi informatsii ta kiberbezpeka pidpryiemstva" [Protection of accounting information and cybersecurity of the enterprise]. *Ekonomika i suspilstvo*, no. 11 (2017): 497-502.

Von Solms, R., and van Niekerk, J. "From information security to cyber security". Computers & Security. 2013. https://www.sciencedirect.com/science/article/pii/S0167404813000801?via%3Dihub

Yevtushevska, O. A. "Informatsiina bezpeka yak element pidvyshchennia efektyvnosti kompleksnoho kontroliu pidpryiemstv vodnoho transportu" [Information security as an element of increasing the efficiency of integrated control of water transport enterprises]. *Zovnishnia torhivlia: ekonomika, finansy, pravo*, no. 5-6 (2015): 157-162.