УДК 657:338.45

DOI: https://doi.org/10.32841/2413-2675/2019-40-23

Ілляшенко К.В.
к.е.н., доцент,
доцент кафедри обліку і оподаткування,
Таврійський державний агротехнологічний університет
імені Дмитра Моторного
Illiashenko Kateryna
Dmytro Motornyi Tavria State Agrotechnological University

ІНФОРМАЦІЙНА БЕЗПЕКА СУЧАСНОГО БУХГАЛТЕРСЬКОГО ОБЛІКУ

INFORMATION SECURITY OF MODERN ACCOUNTING

Анотація. У публікації розглянуто питання впливу інформаційних технологій на економічну безпеку діяльності підприємства в сучасних умовах господарювання. Досліджено найбільш поширені підходи до визначення економічної безпеки підприємства. Висвітлено поняття «інформаційні загрози» та «інформаційна безпека» як окремі категорії, що найбільш притаманні автоматизованим виробничим та обліково-аналітичним процесам. Визначено види інформаційного ризику як у конкретних випадках, так і у широкому контексті інформаційної безпеки. Проаналізовано рівень ризиків інформаційної загрози та способи їх оцінки. Обґрунтовано доцільність інформаційної безпеки під час ведення бухгалтерського обліку з використанням комп'ютерних технологій. Запропоновано заходи щодо попередження ймовірних інформаційних небезпек для обліково-аналітичної діяльності.

Ключові слова: інформація, інформаційні технології, безпека, підприємство, ризики, діяльність, бухгалтерський облік.

Постановка проблеми. Швидке вдосконалювання інформатизації, її проникнення в усі сфери суспільства та держави викликали, крім безсумнівних переваг, і появу низки суттєвих проблем. Однією з них стала необхідність захисту підприємства від імовірних інформаційних небезпек. Тоді як економічний потенціал усе більшою мірою визначається рівнем розвитку інформаційної структури, пропорційно зростає й потенційна уразливість економіки від інформаційних впливів. Хакерські атаки, віруси-вимагачі, промислове шпигунство, крадіжка персональної інформації – усе це стало невід'ємною частиною ризиків для діяльності підприємств. А повністю автоматизована форма бухгалтерського обліку з підключенням до мережі стає одним з основних джерел подібної уразливості.

Аналіз останніх досліджень і публікацій. В основі дослідження питань економічної безпеки були використані роботи І. Шевченка, Н. Лоханової, Ю. Боснера та ін. Вирішення проблеми інформаційної безпеки та інформаційних ризиків започатковано в працях О.В. Царєгородцева, В.М. Цигічка, В.М. Ясенєва тощо. Проблеми інформаційної безпеки бухгалтерського обліку розглядалися у дослідженнях В. Муравського, Н.Л. Шишкової, М.М. Ігнатенко.

Виділення не вирішених раніше частин загальної проблеми. Незважаючи на велику кількість публікацій із досліджуваної проблеми, дотепер відсутній комплексний аналіз потенційних інформаційних загроз бухгалтерському обліку на підприємствах.

Мета статті. Головною метою цієї роботи є розгляд питання впливу інформаційних технологій на економічну безпеку діяльності підприємства, аналіз інформаційних ризиків для ведення бухгалтерського обліку та пошук заходів щодо попередження ймовірних інформаційних небезпек.

Виклад основного матеріалу. Формування інформаційного суспільства опирається на

новітні інформаційні, телекомунікаційні технології та технології зв'язку. Саме нові технології призвели до бурхливого поширення глобальних інформаційних мереж, що відкривають принципово нові можливості міжнародного інформаційного обміну. Формування інформаційного суспільства концептуально та практично означає формування нового світогляду, в якому дуже велике значення матиме безпека від інформаційних загроз.

Інформатизація економіки розпочалася не так давно з упровадженням обчислювальної техніки та поширенням мережі Інтернет. Вона поставила низку нових питань перед дослідниками економічної діяльності підприємств, у тому числі з питань економічної безпеки.

Можна виділити кілька поширених підходів до визначення економічної безпеки підприємства:

– захист від економічних злочинів – забезпечення безпеки підприємства зводять до захисту від різного роду економічних злочинів (крадіжки, шахрайство, фальсифікації, промислове шпигунство тощо). Звичайно, ці загрози дуже важливі та повинні постійно аналізуватися й ураховуватися, але зводити поняття економічної безпеки тільки до цього не можна [1, с. 179];

– стан ефективного використання ресурсів або потенціалу – підхід, що намагається уникнути вживання поняття загрози у визначенні економічної безпеки, базується на економічних поняттях досягнення мети, функціонування підприємства, тобто є ресурсно-функціональним підходом;

– наявність конкурентних переваг – підхід, послідовники якого вважають, що наявність конкурентних переваг, зумовлених відповідністю матеріального, фінансового, кадрового, технологічного потенціалів та організаційної структури підприємства його стратегічним цілям і завданням забезпечать йому певний рівень економічної безпеки [2, с. 54]. Але сам факт наявності переваг і потенціалу без їх використання та реалізації не гарантує підприємству економічної безпеки;

– реалізація та захист економічних інтересів – відносно новий підхід, заснований на реалізації та захисті економічних інтересів підприємства, визначає економічну безпеку як захищеність його життєво важливих інтересів від внутрішніх і зовнішніх загроз, тобто захист підприємства, його кадрового й інтелектуального потенціалу, інформації, технологій, капіталу та прибутку, що забезпечується системою заходів спеціального правового, економічного, організаційного, інформаційно-технічного та соціального характеру [3, с. 37].

На нашу думку, найбільш правильним є останній підхід, тому що у ньому нарівні з іншими оговорюється система заходів інформаційно-технічного характеру. Але інформаційні загрози поки що не виділяються в окрему категорію.

Оскільки об'єктом інформаційної безпеки є підприємство, зміст поняття інформаційної безпеки буде полягати у захищеності інтересів власника даного підприємства, що задовольняють за допомогою інформації або пов'язаних із захистом від несанкціонованого доступу тих відомостей, які уявляються власникові досить важливими. Інтереси проявляються через об'єкти, здатні служити для їхнього задоволення, і дії, що вживають для володіння цими об'єктами. Відповідно, інтереси як об'єкт безпеки можуть бути представлені сукупністю інформації, здатної задовольняти інтерес власника, і його дій, спрямованих на оволодіння інформацією або приховування інформації. Ці складники об'єкта інформаційної безпеки й захищаються від зовнішніх і внутрішніх загроз [4, с. 188].

Зазначимо, що застосування інформаційних технологій є одним із важливих чинників, що визначають конкурентоздатність підприємств. Однак поряд з очевидними перевагами, такими як автоматизація виробничих і обліково-аналітичних процесів, доступність електронних розрахунків, швидкість обробки інформації для прийняття управлінських рішень, використання інформаційних технологій привносить нові істотні ризики [5, с. 20].

Можна привести багато визначень інформаційних ризиків, використання кожного з яких буде виправдано розв'язуваними завданнями. Саме вузьке визначення інформаційних ризиків – це ризики втрати, несанкціонованої зміни інформації через збої у функціонуванні інформаційних систем або їх виходу з ладу, що приводять до збитків. У цьому разі інформаційний ризик відповідає категорії та рівню

операційних ризиків у класифікації Базельського комітету «Зупинка бізнесу та збої у системах». Найбільш широке визначення включає ризик виникнення збитків через неправильну організацію або навмисне порушення інформаційних потоків і систем організації. Таке розуміння інформаційного ризику виправдано, якщо оцінювати ризики в широкому контексті інформаційної безпеки [6, с. 251].

Відповідно до базельської класифікації категорій подій і прикладів дій, які можуть призводити до реалізації операційних ризиків, до інформаційних ризиків можна віднести зазначені у табл. 1.

Інформаційні технології допомагають в управлінні та оптимізації діяльності підприємства, запобігають багатьом економічним ризикам, наприклад знижують вірогідність банкрутства [8, с. 197]. Але водночас вони ж виступають і фактором ризику.

Питання інформаційної безпеки під час ведення бухгалтерського обліку з використанням комп'ютерних технологій доцільно розглядати у двох аспектах: запобігання зловживанням чи ненавмисним порушенням працівниками підприємства (внутрішній аспект) та створення належної інформаційної безпеки для запобігання несанкціонованому доступу, пошкодженню комп'ютерних програм чи даних вірусами, комп'ютерному саботажу (зовнішній аспект) [9, с. 232].

Превентивні механізми запобігання втратам та перекрученням облікової інформації повинні базуватися на комплексних, взаємопов'язаних методиках і процедурах виявлення, аналізу ризиків для інформаційної системи обліку підприємства, розробленні контрольних технологій щодо управління безпекою облікової інформації [10, с. 126].

Сьогодні найбільшу питому вагу в цій групі заходів у системах обробки обліково-звітної інформації становлять спеціальні пакети програм або окремі програми, які включаються до складу програмного забезпечення з метою реалізації завдань щодо захисту інформації. Технологічні засоби інформаційної безпеки – це комплекс заходів, які органічно вбудовуються в технологічні процеси перетворення даних [11, с. 87].

Можливі методи зниження інформаційного ризику для кожної одиниці стандартні і можуть бути використані в обліково-аналітичній діяльності [12, с. 121]:

- прийняття ризику – визнання потенційних утрат прийнятними;
- запобігання ризику – прийняття рішень, спрямованих на видалення фактора ризику, зокрема усунення причин відповідної загрози

Таблиця 1

Категорії подій і рівні інформаційних ризиків

Рівень ризику	Категорія подій виникнення ризику	Приклади дії ризику
1-й	Внутрішнє шахрайство	Несанкціоноване використання інформаційних систем Навмисне перекручування (приховування/розкриття) важливої інформації, що призвело до грошових утрат
2-й	Зовнішнє шахрайство	Незаконне проникнення в інформаційні системи, у тому числі за допомогою мережі Інтернет Заподіяння збитку інформаційним системам Крадіжка інформації, що призвела до грошових утрат
3-й	Клієнти, продукти та ведення бізнесу	Пов'язане з недостатністю систем неправомірне розкриття конфіденційної інформації
4-й	Збиток для матеріальних активів	Збиток матеріальним цінностям (у цьому разі інформаційним системам) у результаті впливу зовнішніх «природних» подій Збиток, що нанесено інформаційним системам від актів тероризму, вандалізму тощо
5-й	Зупинка бізнесу та збої у системах	Вихід із ладу інформаційних систем, окремих модулів і елементів її функціонала Відмови та збої у роботі автоматизованих систем Збої у роботі каналів зв'язку Поломка обладнання (комп'ютери, термінали, інше устаткування)
6-й	Проблеми з керуванням і виконанням	Відсутність (недосконалість) системи захисту або порядку контролю доступу до інформації Неправильна організація інформаційних потоків Невиконання зобов'язань перед постачальниками, банками, провайдерами Помилки під час уведення й обробки даних

Джерело: складено на основі [7]

(наприклад, відмова від використання встановленого програмного забезпечення, що істотно порушує вимоги інформаційної безпеки);

- обмеження ризику – впровадження спеціальних засобів контролю, що знижують імовірність реалізації інформаційної загрози та (або) її наслідки;

- передача ризику – створення умов для компенсації потенційних утрат шляхом передачі ризику третій особі, наприклад використовуючи страхування або віддаючи окремі функції на аутсорсинг.

Зазначені способи не є взаємовиключними та можуть застосовуватися комплексно.

Але запобігання інформаційним небезпекам не повинно зводитися до одного тільки зниження ризиків. Оскільки настання кризових ситуацій практично неможливо прогнозувати, необхідно створити цілу низку заходів, передусім систем контролю, для швидкого реагування та прийняття вірних управлінських рішень.

Для автоматизованої форми обліку дуже важливо мати надійний захист та щоденне резервне копіювання даних на безпечних носіях. Не повинна вважатися застарілою роздруківка найбільш важливих фінансових документів на папері, щоб робота бухгалтерської служби не припинялася, наприклад через перебої електроенергії.

На нашу думку, не менш важливим чинником безпеки бухгалтерського обліку є використання лише ліцензованого програмного забезпечення, яке має службу технічної підтримки, оновлення уразливих компонентів тощо.

Також проблема заслуговує більш уважного відношення від керівників підприємств, які все ще використовують застарілі моделі управління. Формування нового підходу потребує перегляду кадрових питань, нових форм контролю й обов'язкового урахування чинників, що притаманні новій цифровій економіці.

Висновки і пропозиції. У ході дослідження нами зроблено висновок, що на даному етапі інформаційні загрози є недооціненими та недостатньо вивченими у розрізі облікової діяльності підприємств. Тоді як економічний потенціал усе більшою мірою визначається рівнем розвитку інформаційної структури, пропорційно зростає й потенційна уразливість економіки від інформаційних впливів. Тому так важливо всебічно вивчити види інформаційних загроз і розробити заходи щодо їх уникнення. Це передусім формування нового підходу до управління підприємством, захисту внутрішньої інформації від зовнішнього втручання, аналіз інформаційних ризиків під час прийняття управлінських рішень тощо.

Науково-технічний прогрес призвів до того, що інформаційне середовище зростає у геометричній прогресії й інформаційні технології проникають у всі сфери життя. Інформаційні аспекти безпеки облікової та іншої діяльності підприємств стають усе більш пріоритетними. Таким чином, тематика інформаційних загроз та безпеки бухгалтерського обліку залишається досить актуальною, а розглянуті питання заслуговують на подальші поглиблені дослідження.

Література:

1. Шевченко І. Особливості формування економічної безпеки підприємства. *Наука молода.* 2010. № 10. С. 178–181.
2. Лоханова Н. Система управління станом економічної безпеки підприємства: проблемні питання, концепція розвитку. *Економіст*. 2005. № 2. С. 52–56.
3. Боснер Ю. Стратегические подходы к экономической безопасности предприятий. *Институциональная экономика.* 2010. № 1. С. 34–48.
4. Аналіз нормативно-правових та організаційно-технічних аспектів забезпечення інформаційної безпеки / В.В. Овсянніков та ін. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2015. № 3(24). С. 187–193.
5. Ткачук Т. Формування системи інформаційної безпеки бізнесу. *Бізнес і безпека.* 2009. № 4. С. 19–23.
6. Міщенко С.П. Інформаційна складова економічної безпеки підприємства. *Вісник економіки транспорту і промисловості.* 2012. № 39. С. 250–254.
7. International Convergence of Capital Measurement and Capital Standards A Revised Framework, Basel, Switzerland, November 2005.
8. Терещенко М.А. Інформаційні технології в системі управління підприємством та запобігання його банкрутству. *Збірник наукових праць Таврійського державного агротехнологічного університету (економічні науки).* 2012. № 1(17). С. 193–200.
9. Муравський В. Забезпечення інформаційної безпеки в автоматизованих системах бухгалтерського обліку. *Економічний аналіз.* 2013. Вип. 12. Ч. 4. С. 232–235.
10. Шишкова Н.Л. Засоби підвищення керованості безпекою облікової інформації. *Економічний вісник.* 2016. № 3. С. 119–127.
11. Ігнатенко М.М. Формування інформаційної безпеки підприємств і організацій в умовах автоматизації обліку та фінансової звітності. *Вісник Бердянського університету менеджменту і бізнесу.* 2017. № 4(40). С. 84–88.
12. Ілляшенко К.В. Інформаційний взаємозв'язок аналізу та бухгалтерської звітності. *Вісник ХНТУСГ. Економічні науки.* 2012. № 127. С. 118–123.

References:

1. Shevchenko I. (2010) Osoblyvosti formuvannia ekonomichnoi bezpeky pidpryiemstva [Features of formation of economic security of the enterprise]. *Nauka moloda*. no. 10. pp. 178–181.
2. Lokhanova N. (2005) Systema upravlinnia stanom ekonomichnoi bezpeky pidpryiemstva: problemni pytannia, kontseptsiia rozvytku [Management system of the state of economic security of the enterprise: problematic issues, the concept of development]. *Ekonomist*. no. 2. pp. 52–56.
3. Bosner Yu. (2010) Strategicheskie podhodyi k ekonomicheskoy bezopasnosti predpriyatiy [Strategic approaches to economic security of enterprises]. *Institutsionalnaya ekonomika.* no. 1. pp. 34-48.
4. Ovsiannikov V.V., Dekhtiar S.V., Palamarchuk S.A., Chernysh Yu.O., Shemendiuk O.V. (2015) Analiz normatyvno-pravovykh ta orhanizatsiino-tekhnichnykh aspektiv zabezpechennia informatsiinoi bezpeky [Analysis of legal, organizational and technical aspects of information security]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony.* no. 3(24). pp. 187–193.
5. Tkachuk T. (2009) Formuvannia systemy informatsiinoi bezpeky biznesu [Formation of business information security system]. *Biznes i bezpeka.* no. 4. pp. 19–23.
6. Mishchenko S.P. (2012) Informatsiina skladova ekonomichnoi bezpeky pidpryiemstva [Information component of economic security of the enterprise]. *Visnyk ekonomiky transportu i promyslovosti.* no. 39. S. 250–254.
7. International Convergence of Capital Measurement and Capital Standards A Revised Framework, Basel, Switzerland, November 2005.
8. Tereshchenko M.A. (2012) Informatsiini tekhnolohii v systemi upravlinnia pidpryiemstvom pidpryiemstva ta zapobihannia yoho bankrutstva [Information technologies in the enterprise management system of the enterprise and prevention of its bankruptcy]. *Zbirnyk naukovykh prats Tavriiskoho derzhavnoho ahrotekhnolohichnoho universytetu (ekonomichni nauky)*. no. 1(17). pp. 193–200.
9. Muravskyi V. (2013) Zabezpechennia informatsiinoi bezpeky v avtomatyzovanykh systemakh bukhhalterskoho obliku [Information security in automated accounting systems]. *Ekonomichnyi analiz.* Vol. 4. no. 12. pp. 232–235.
10. Shyshkova N.L. (2016) Zasoby pidvyshchennia kerovanosti bezpekoiu oblikovoi informatsii [Tools to improve security manageability of accounting information]. *Ekonomichnyi visnyk.* no. 3. pp. 119–127.
11. Ignatenko M.M. (2017) Formuvannia informatsiinoi bezpeky pidpryiemstv i orhanizatsii v umovakh avtomatyzatsii obliku ta finansovoi zvitnosti [Formation of information security of enterprises and organizations in the conditions of authorization of accounting and financial statements]. *Visnyk Berdianskoho universytetu menedzhmentu i biznesu.* no. 4(40). pp. 84–88.
12. Illiashenko K.V. (2012) Informatsiinyi vzaiemozviazok analizu ta bukhhalterskoi zvitnosti [The information relationship analysis and financial statements]. *Visnyk KhNTUSH: ekonomichni nauky*. no. 127. pp. 118–123.

Аннотация. В публикации рассмотрены вопросы влияния информационных технологий на экономическую безопасность деятельности предприятия в современных условиях хозяйствования. Исследованы наиболее распространенные подходы к определению экономической безопасности предприятия. Освещены понятия «информационные угрозы» и «информационная безопасность» в качестве отдельных категорий, наиболее свойственных автоматизированным производственным и учетно-аналитическим процессам. Определены виды информационного риска как в конкретных случаях, так и в широком контексте информационной безопасности. Проанализированы уровень рисков информационной угрозы и способы их оценки. Обоснована целесообразность информационной безопасности при ведении бухгалтерского учета с использованием компьютерных технологий. Предложены меры по предупреждению вероятных информационных опасностей для учетно-аналитической деятельности.

Ключевые слова: информация, информационные технологии, безопасность, предприятие, риски, деятельность, бухгалтерский учет.

Summary. The purpose of the study is to consider the impact of information technology on the economic security of the enterprise, the analysis of information risks for accounting and the search for measures to prevent possible information hazards. The formation of the information society conceptually and practically means the creation of a new worldview in which protection from information threats will be very important. The article discusses the impact of information technology on the economic security of the enterprise in modern economic conditions. The most common approaches to the definition of economic security of the enterprise are investigated. The concepts of «information threats» and «information security» as separate categories, the most characteristic of automated production and accounting and analytical processes, are highlighted. The types of information risk, both in specific cases and in the broad context of information security, are defined. The level of risks of information threat and ways of their estimation are analyzed. The expediency of information security in accounting with the use of computer technologies is substantiated. It was agreed that the issues of information security in accounting with the use of computer technology should be considered in two aspects: prevention of abuse or unintentional violations by employees of the enterprise (internal aspect) and the creation of appropriate information security to prevent unauthorized access, damage to computer programs or data viruses, computer sabotage (external aspect).The measures on prevention of probable danger for information that serves for accounting and analytical activity are offered, such as possible methods of reduction of information risk, formation of a new approach to enterprise management, protection of internal information from external interference, analysis of information risks at decision-making of management decisions. It is concluded that the formation of a new approach to information security of accounting requires a review of personnel issues, new forms of control and mandatory accounting of factors characteristic of the new digital economy.

Keywords: information, information technology, security, enterprise, risks, activities, accounting.