УДК 657:004.056

Захист облікової інформації та кібербезпека підприємства

Вітер С.А.
кандидат педагогічних наук, старший викладач
Житомирського національного агроекологічного університету

Світлишин І.І.
кандидат економічних наук, доцент,
Житомирський національний агроекологічний університет

У статті розглянуто визначення дефініцій «захист облікової інформації», «безпека», «кібербезпека», «кіберпростір», розкрито відмінність між інформаційною та кібербезпекою, запропоновано авторське бачення поняття «кібербезпека облікової інформації». Обґрунтовано актуалізацію питання організації на підприємствах системи кібербезпеки облікової інформації. Визначено принципи і заходи щодо захисту облікової інформації в контексті кібербезпеки та деякі аспекти її організації.

Ключові слова: безпека, кібербезпека, кіберпростір, захист облікової інформації, загрози.

Витер С.А., Светлишин И.И. ЗАЩИТА УЧЕТНОЙ ИНФОРМАЦИИ И КИБЕРБЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

В статье рассмотрены определения дефиниций «защита учетной информации», «безопасность», «кибербезопасность», «киберпространство», раскрыто различие между информационной и кибербезопасностью, предложено авторское видение понятия «кибербезопасность учетной информации». Обоснована актуализация вопроса организации на предприятиях системы кибербезопасности учетной информации. Определены принципы и меры по защите учетной информации в контексте кибербезопасности и некоторые аспекты ее организации.

Ключевые слова: безопасность, кибербезопасность, киберпространство, защита учетной информации, угрозы.

Viter S.A., Svitlyshyn I.I. PROTECTION OF ACCOUNTING INFORMATION AND CYBER SECURITY OF THE ENTERPRISE

In the article definitions of definitions «protection of accounting information», «security», «cybersecurity», «cyberspace» are considered, the distinction between information and cybersecurity is revealed, author's vision of the concept «cybersecurity of accounting information» is offered. It is justified to actualize the issue of organization of accounting information at enterprises of the cybersecurity system. The principles and measures for the protection of accounting information in the context of cybersecurity and certain aspects of its organization are defined.

Keywords: security, cybersecurity, cyberspace, protection of accounting information, threats.

Постановка проблеми у загальному вигляді. Протягом останніх років все ширше використання перспективних IT-технологій зумовило не лише численні переваги, а й цілу низку проблем. Зокрема, істотно підвищився рівень інформаційного негативного впливу на процеси збереження та розповсюдження інформації, зросла чисельність нових загроз інформаційній безпеці, таких як нові форми кібератак.

Гарантування стабільного максимально ефективного функціонування та розвитку будь-якого підприємства є основним завданням безпеки його економічної інформації. Найціннішою економічною інформацією є облікова інформація, яка характеризує всі аспекти господарської діяльності. Сьогодні більшість суб'єктів господарювання використовують комп'ютеризовану форму ведення бухгалтерського обліку, яка передбачає використання спеціалізованого програмного забезпечення та технічних засобів. При цьому в комп'ютерних системах зберігаються і обробляються великі обсяги облікової інформації, будь-який збій може привести до надмірних витрат, недостатніх доходів, втрати активів, санкцій тощо. Тому головним пріоритетом захисту облікової інформації на підприємстві є розроблення заходів, спрямованих на збереження інформації, що міститься у комп'ютерних базах підприємства.

С.М. Деньга та Ю.А. Верига виділяють такі дві категорії загроз комп'ютерним інформаційним системам бухгалтерського обліку, як активні і пасивні. Активні загрози включають комп'ютерне шахрайство та комп'ютерний саботаж. Пасивні загрози – це помилки сис-

теми (пошкодження окремих компонентів обладнання) та катастрофи [7]. Дослідники вказують, що 45% причин виникнення кризового стану становлять навмисні дії.

У зв'язку з тим, що останнім часом збільшується кількість незаконних фінансових операцій, крадіжок та шахрайства в мережі Інтернет, несанкціонованого використання чи модифікації програмного забезпечення, під час оцінки надійності систем інформаційної безпеки мають бути змінені пріоритети від забезпечення традиційної інформаційної безпеки до кібербезпеки.

Питання кібербезпеки зачіпає інтереси не лише державних інституцій, а і приватного сектору та громадянського суспільства. При цьому низький рівень взаємодії органів державної влади, неурядових організацій та приватного сектору, а також відсутність системних нормативних документів, які описували б загрози Україні в кіберпросторі, є наслідком відсутності цілісного обговорення кібербезпекових питань.

Аналіз останніх досліджень та публікацій. Над розв'язанням проблеми забезпечення інформаційної безпеки підприємств працювали А.П. Дикий, О.І. Захаров, Е.Е. Ібрагімов, Н.С. Іванова, О.О. Мельник, М.В. Наконечна, О.В. Орлик, Л.С. Сорока, В.Н. Ясенів. Різні аспекти захисту облікової інформації розглядали І.В. Горячківська, В.В. Євдокимов, І.Ю. Кравченко, Н.Л. Шишкова, В.А. Шпак та ін. Питання визначення загроз кібербезпеки під час захисту облікової інформації знайшли відображення у роботах Ю.Ю. Мороз, Ю.С. Цаль-Цалка, В.В. Сторож. Однак проблеми забезпечення кібербезпеки облікової інформації підприємств залишаються мало дослідженими.

Формулювання цілей статті (постановка завдання). Метою статті є висвітлення необхідності та змісту організації захисту облікової інформації у контексті забезпечення кібербезпеки підприємства.

Виклад основного матеріалу дослідження. Під захистом облікової інформації розуміється стан її захищеності від випадкових або навмисних впливів природного або штучного характеру, що можуть привести до нанесення шкоди власникам або користувачам цієї інформації. Якщо розглядати це поняття без конкретики, то можна говорити про інформаційну безпеку загалом. Однак коли захист інформації стосується забезпечення безпеки інформаційних баз даних, а також різних програм, що входять у комп'ютерні мережі, виникає необхідність визначити співвідношення між інформаційною безпекою та кібербезпекою.

Фахівці з комп'ютерної безпеки вважають, що кібербезпека – це лише новий термін, який визначає саме те, чим вони займалися протягом останніх десятиліть. Інший науковий погляд на сутність кібербезпеки означає наступальні дії, тобто кібербезпека відрізняється від традиційної інформаційної безпеки тим, що вона включає застосування практичних дій і засобів для атаки супротивників.

У науковій літературі під час розмежування понять «кібербезпека» та «інформаційна безпека» загрози кібербезпеці визначаються в уразливості об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, а також у фізичній і моральній застарілості системи охорони державної таємниці та інших видів інформації з обмеженим доступом. О.А. Баранов вважає, що проблема оцінки стану кібербезпеки повинна розглядатися у нерозривному зв'язку з оцінкою можливих чи завданих збитків соціальним або соціотехнічним системам як системам більш високого порядку [1, с. 60].

Можна погодитися з тим, що на відміну від інформаційної безпеки мова йде не про інформацію взагалі, а про ту інформацію, яка циркулює в кіберпросторі і становить важливу частину її змісту. Зрозуміло, що втрата інформації, яка зберігається в окремому комп'ютері і є важливою для користувача цього комп'ютера, не може розглядатися як загроза кібербезпеці. Однак захист інформації потрібно передбачувати, виходячи із цінності інформації не для себе, а для зловмисників, які будують відносини винятково на грошовій основі. Привабливою може бути інформація управлінського обліку, яка містить комерційну таємницю.

Стає очевидним, що питання кібербезпеки мають бути у порядку денному кожного підприємства незалежно від його масштабів, рівня складності і характеру комерційної діяльності, а також усвідомлені усіма співробітниками підприємства. Розробники «Настанови з кібербезпеки від експертів» звертають увагу на те, що, як правило, більшу ініціативу щодо зниження ризиків, які надходять від кіберзагроз, проявляють великі міжнародні компанії, хоча ті самі загрози та ризики рівною мірою поширюються також на представників середнього і сімейного бізнесу [11].

Із позицій міжнародної організації «Міжнародний телекомунікаційний союз» (International Telecommunication Union, ITU) кібербезпека – це набір засобів, стратегії, принципи забезпе-

чення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача [13].

У визначення «кібербезпека» за основу покладаємо розуміння поняття «безпека», що згідно з українським тлумачним словником означає стан, коли кому-небудь або чому-небудь ніщо не загрожує [14]. Відповідно кібербезпека – це деякий стан системи, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах.

Вітчизняні науковці висловлюють думку про те, що проблему кіберзлочинності загострює відставання нормативного регулювання цієї сфери в Україні від розвитку нових інформаційних технологій.

У національній стратегії кібербезпеки України розкривається поняття забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів.

При цьому під кіберпростором розуміється середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [12].

М.М. Безкоровайний, А.Л. Татузов кіберпростір розглядають як тріаду, яка містить у собі три основні складники, такі як 1) інформація в її цифровому поданні – статичному (файли, записані на носії даних) і динамічному (пакети, потоки, команди, запити); 2) технічна інфраструктура, ІКТ, програмне забезпечення, за допомогою яких здійснюється реалізація основних дій з інформацією (Інтернет і мережеві взаємозв'язки, комп'ютери, гаджети тощо); 3) інформаційна взаємодія суб'єктів із використанням інформації, одержуваної і оброблюваної за допомогою технічної інфраструктури [2, с. 24]. Вважаємо за необхідне до перелічених складників віднести відповідне реагування на загрози, тобто практичні дії та засоби зворотного впливу на атакуючі сторони.

Дотримуємося погляду на розуміння кіберпростору як віртуального комунікаційного середовища, утвореного системою зв'язків між користувачами та об'єктами інформаційної інфраструктури, такими як електронний інформаційний ресурс (ІР), системи й мережі всіх форм власності, керовані автоматизованими системами управління, що використовуються не лише для перетворення та передавання інформації, котра в них циркулює, з метою забезпечення інформаційних потреб суспільства, а й для впливу на аналогічні об'єкти протиборчої сторони [4].

Кібербезпеку в частині облікової політики підприємства, засновану на реалізації і захисті економічних інтересів підприємства, Ю.Ю. Мороз та Ю.С. Цаль-Цалко визначають як захищеність його життєво важливих інтересів від внутрішніх і зовнішніх загроз, тобто захист підприємства, його кадрового і інтелектуального потенціалу, інформації, технологій, прибутку, доданої та ринкової вартості підприємства, який забезпечується системою заходів спеціального правового, економічного, організаційного, інформаційно-технічного і соціального характеру [16, с. 9].

З огляду на сутність поняття «захист інформації», яке трактується міжнародним стандартом ISO/IEC 27001 як забезпечення конфіденційності, цілісності та доступності інформації [9], під кібербезпекою облікової інформації розуміємо стан її захищеності, що створюється, зберігається, змінюється та використовується за допомогою комп'ютерної техніки, за якого забезпечується своєчасне виявлення, запобігання і нейтралізація несанкціонованого використання облікової інформації, порушення її конфіденційності, цілісності або знищення через електронні засоби, що ставить під загрозу життєво-важливі економічні інтереси підприємства.

Завдання організації кіберзахисту і безпеки даних у бухгалтерії полягає у забезпеченні комплексу організаційно-технічних заходів та кадрової роботи, спрямованої на збереження комерційної таємниці. Відповідно до цього вважаємо, що всі заходи щодо кіберзахисту облікової інформації можна умовно поділити на три групи (рис. 1). Більшість засобів захисту реалізуються у вигляді програм або пакетів програм, що розширюють можливості стандартних операційних систем, а також систем керування базами даних.

До суто технічних засобів захисту бухгалтерської інформації в автоматизованій системі науковці відносять шифрування документів [8, с. 136; 3, с. 22]. На технологічному рівні заходами з кібербезпеки можуть бути контроль доступу до облікових даних, управління та безпека авторизації облікової інформації.

Основним способом попередження кіберзагроз є впровадження послідовних рівнів заходів контролю за доступом до сайту, системи та файлів. Створення механізму підзвітності дає змогу визначати, хто працює в системі та що робить у певний момент часу, і протоколювати події, що відбувалися в комп'ютерній інформаційній системі бухгалтерського обліку. Деякі засоби захисту передбачає програмне забезпечення бухгалтерського обліку. Так, у програмних продуктах «Парус-Підприємство», «1С:Підприємство» така система має вигляд паролю для входу в програму. Бухгалтерська система «1С:Підприємство. Версія 7.7» дає власникам можливості розмежування доступу до функцій та файлів, до окремих ділянок обліку, встановлення паролів користувачів, фіксування авторства створених документів, ведення журналу реєстрації роботи з програмою, визначення прав на видалення документів і записів з інформаційної бази.

Крім застосування засобів захисту, що вбудовуються у програмне забезпечення, повинна бути передбачена низка адміністративних заходів, наприклад, стеження за відсутністю підслуховуючих пристроїв у комп'ютерних мережах тощо. При цьому важливими складниками захисту є компетентність та суворе виконання зобов'язань щодо гарантій дотримання необхідних правил безпеки облікового персоналу, від коректності дій якого залежить рівень кібербезпеки підприємства.

Вивчаючи роль бухгалтера у системі забезпечення економічної безпеки підприємства, Т.В. Давидюк та К.П. Боримська зазначають, що не меншу роль відіграє обізнаність облікових працівників у системі захисту економічної безпеки окремого суб'єкта господарювання [6]. Є доцільною практика заохочування постачальників та підрядників до дотримування принципів захисту інформації підприємства, яке замовляє продукцію, товари, роботи, послуги.

О.А. Клименко некомпетентними діями працівників, які є загрозою втрати інформації, називає:

– відкриття на своєму комп'ютері файлів, надісланих електронною поштою або програмами миттєвого обміну повідомленнями від невідомих адресатів;

– встановлення неліцензійного програмного забезпечення, не потрібного для виконання функціональних обов'язків працівника;

– використання паролів «за замовчуванням», створення простих паролів або небажання змінювати паролі протягом тривалого часу, «запам'ятовування» пароля у вікнах уведення, особливо на комп'ютерах для публічного доступу;

– роботу з конфіденційними документами у місцях публічного доступу;

– повідомлення по телефону будь-яких даних про обліковий запис, логіни, паролі;

– нецільове використання мережевих ресурсів тощо [10].

Очевидно, що об'єктом зацікавленості злочинців була і завжди буде приватна інформація, витоки якої здійснюють під час використання соціальних мереж через такі канали, як персональні комп'ютери, ноутбуки, смартфони, а тому підприємствам необхідно прописувати правила користування цією інформацією і стежити за безумовним їх виконанням.

Не менш важливим повинно стати належне реагування на інциденти (внутрішнє чи зовнішнє – залежно від обставин). Інформування відповідних органів є способом поліпшення загальної ситуації у галузі кібербезпеки.

Отже, ефективність системи кібербезпеки залежить від ефективного управління ризиками. Загалом управління кібербезпекою входить до загальної системи управління еконо-

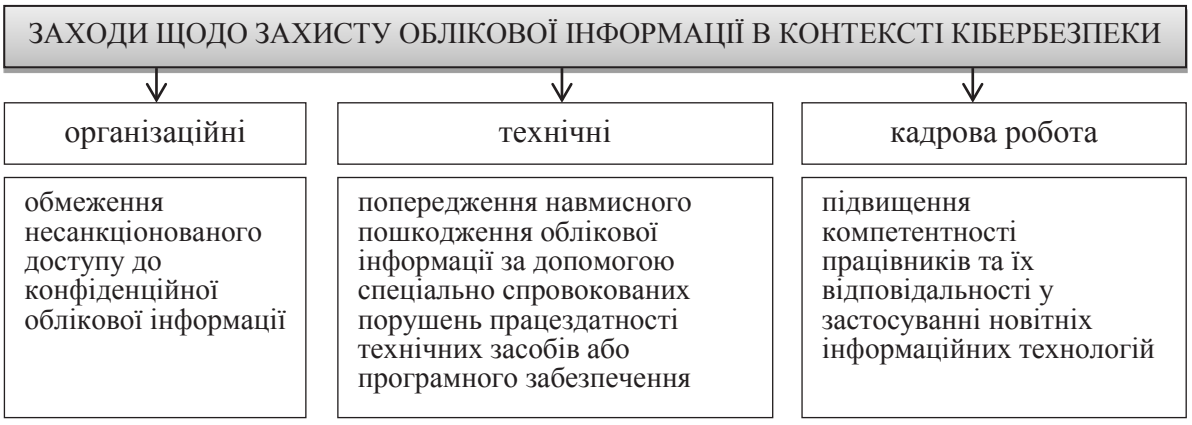

Рис. 1. Заходи щодо кіберзахисту облікової інформації

мічною безпекою підприємства, і залежно від розмірів та потужності підприємства, а також відповідно до розрахунків економічної доцільності рівня захисту облікової інформації вирішуються організаційно-кадрові питання. Вони передбачають створення або спеціальної служби із забезпечення кібербезпеки облікової інформації, або введення посади спеціаліста з кібербезпеки, який займатиметься розробленням охоронних систем для різних комунікаційних мереж і електронних баз даних у структурі служби внутрішнього контролю підприємства або бухгалтерської служби.

Спецслужбу з кібербезпеки можуть представляти фахівці з організації інформаційної безпеки та проведення тестування на проникнення, інспектори з організації захисту секретної інформації, аналітики проектів із кібербезпеки, системні адміністратори, адміністратори комп'ютерних мереж, менеджери систем з інформаційної безпеки, аналітики систем забезпечення кібербезпеки.

Обов'язками таких фахівців є:

– виявлення уразливих місць системи та моделювання можливої ситуації стороннього кібервпливу з позиції загроз і пов'язаних із ними ризиків;

– контроль надійності функціонування системи захисту облікової інформації, розроблення заходів безпеки на випадок непередбачуваних подій;

– віднесення облікової інформації до категорії обмеженого доступу (службової і комерційної таємниць, іншої конфіденційної інформації);

– розроблення положень, політики і процедур у рамках системи безпеки облікової інформації;

– упровадження розроблених заходів безпеки та випробування системи з оцінкою її результативності, за необхідності внесення коригувань;

– встановлення користувачам комп'ютерної системи бухгалтерського обліку необхідних реквізитів захисту;

– навчання користувачів комп'ютерної інформаційної системи правилам безперервної обробки інформації;

– контроль за дотриманням користувачами комп'ютерної інформаційної системи та персоналом підприємства встановлених правил роботи з обліковою інформацією, що захищається у процесі її автоматизованої обробки.

Для унеможливлення неправомірного втручання у комп'ютерну інформацію та попередження злочинів із його використанням необхідно створити належну систему захисту цієї інформації. Це завдання не може бути вирішене ефективно без дотримання певних принципів (рис. 2).

В обліковій політиці підприємства на основі аналізу сучасного рівня та динаміки розвитку інформаційних технологій необхідно роз-

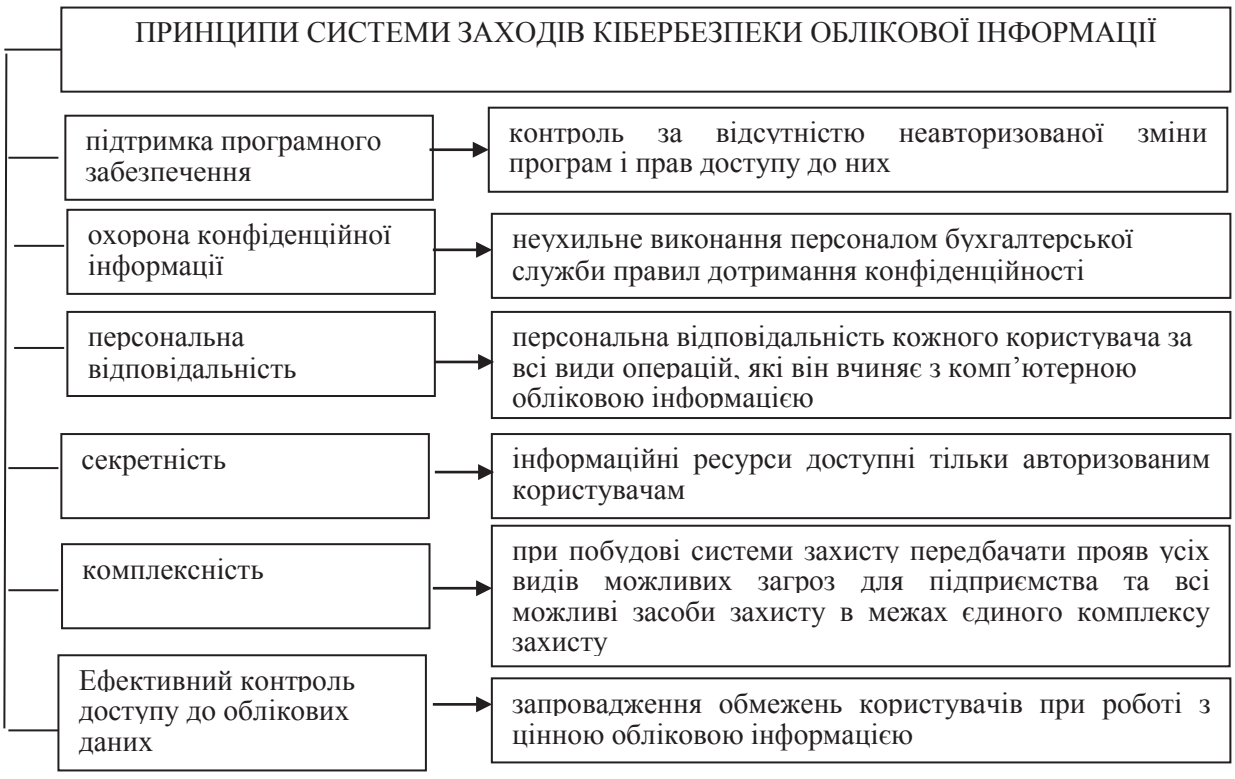

Рис. 2. Основоположні принципи системи заходів кібербезпеки облікової інформації

глядати систематизоване викладення цілей, завдань та принципів досягнення потрібного рівня кібербезпеки облікової інформації підприємства. При цьому варто пам'ятати, що успішний кіберзахист потребує витрат. Фундаментальним питанням, яке необхідно передбачити у наказі про облікову політику, має бути те, на що повинні витрачатися гроші для досягнення базового рівня кібербезпеки, зважаючи на динамічний характер загроз.

Загалом, на відміну від придбання традиційних форм оборонних засобів, де наголос робиться на фізичному обладнанні, дієвість кіберзахисту може більше залежати від обміну інформацією, співпраці і координації. Це все – речі, які важко піддаються фізичному виміру.

Висновки з цього дослідження. На жаль, кіберзлочинність постійно вдосконалюється і йде в ногу з технологіями. Це ускладнює виявлення та протидію зазначеним протиправним діям. Тому варто усвідомити, що проблема кібербезпеки – це проблема не лише загальнодержавного рівня, а кожного окремо взятого підприємства. Зрозуміло, що неможливо досягти стовідсоткової безпеки захисту облікових даних. Проте індивідуальна відповідальність кожного працівника бухгалтерської служби є найпершим і найпростішим фактором, який сприяє захисту цінної облікової інформації. Таким чином, на кожному підприємстві повинна бути створена програма визначених дій, спрямованих на створення кіберзахисту облікової інформації, сфера застосування якого поширюється на людські ресурси і не обмежується виняткова технологічними аспектами.

Перспективою подальших досліджень може бути аналіз загроз та сучасних засобів підтримки кібезбезпеки облікової інформації.

ЛІТЕРАТУРА:

1. Деньга С.М Захист інформації в комп`ютерних інформаційних системах бухгалтерського обліку [Текст] / С.М. Деньга, Ю.О. Верига // Бухгалтерський облік і аудит. – 2004. – № 5. – С. 59-65.

2. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» / О.А. Баранов // Правова інформатика. – № 2(42). – 2014. – С. 54-62.

3. Настанови з кібербезпеки від експертів [Електронний ресурс]. – Режим доступу:http://www.isaca.org.ua/index.php/press-center/news/191-translation-of-guidelines-on-cybersecurity

4. Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. – Женева: МСЭ, 2009. – С. 55. – Режим доступу: //www.itu.int/ITU-T/recommendations/rec. aspx?rec=9136&lang=ru

5. Словник української мови: в 11 тт. / АН УРСР. Інститут мовознавства; за ред. І.К. Білодіда. – К.: Наукова думка, 1970-1980. – Т. 1. – С. 137.

6. Про внесення змін до Закону України «Про основи національної безпеки України»: проект Закону України щодо кібернетичної безпеки України від 07.03.13 р. № 2483. – Режим доступу: // www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998

7. Безкоровайный М.М. Кибербезопасность – подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности. – № 1(2). – 2014. – С. 22-27.

8. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015. – 288 с.

9. Цаль-Цалко Ю.С. Облікова політика підприємства та її кібербезпека / Ю.С. Цаль-Цалко, Ю.Ю. Мороз // Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства: збірник наукових праць, том IV, частина І, Житомир: ПП «Рута», 2017 – С. 8-11.

10. ISO/IEC 27001:2013 information security management system standardarrives [Electronicresource]. – 2013. – Accessedmode: http://www.reuters.com

11. Дикий А.П. Організація бухгалтерського обліку як інструмент забезпечення економічної безпеки підприємств: дис. ... канд. екон. наук: 08.00.09 / А.П. Дикий. – Житомир, 2009. – 172 с.

12. Боримська К.П. Концептуалізація захисту бухгалтерської інформації при міжкорпоративному електронному документообороті торговельних підприємств: проблемні аспекти / К.П. Боримська, Н.В. Кінзерська // Вісник ЖДТУ. – 2013. – № 3(65). – С. 16-25.

13. Давидюк Т.В. Позиціонування обліково-аналітичного забезпечення економічної безпеки підприємства в навчальних планах фахівців напряму підготовки «Облік і аудит» / Т.В. Давидюк, К.П. Боримська // Економіка: реалії часу. Науковий журнал. – 2013. – № 3(8). – С. 83-90. [Електронний ресурс] / – Режим доступу: http://economics.opu.ua/ files/archive/2013/n3.html

14. Клименко В. Внутрішні загрози інформаційній безпеці організації / В. Клименко // Вісник НБУ. – 2008. – № 5. – С. 62-63.