Отримано: 27 листопада 2020 р.

Прорецензовано: 06 грудня 2020 р.

Прийнято до друку: 11 грудня 2020 р.

e-mail: lenazelenina@ukr.net

DOI: 10.25264/2311-5149-2020-19(47)-95-102

Скрипник М. І., Григоревська О. О. Організація захисту облікової інформації в умовах забезпечення кібербезпеки. *Наукові записки Національного університету «Острозька академія». Серія «Економіка» : науковий журнал.* Острог : Вид-во НаУОА, вересень 2020. № 19(47). С. 95–102.

УДК: 657.1

JEL-класифікація: D8, M41

ORCID-ідентифікатор: 0000-0002-6205-0754

ORCID-ідентифікатор: 0000-0001-8279-3523

Скрипник Маргарита Іванівна,
доктор економічних наук, професор, завідувач кафедри обліку і аудиту Київського національного університету технологій та дизайну

Григоревська Олена Олександрівна,
кандидат економічних наук, доцент, доцент кафедри обліку і аудиту Київського національного університету технологій та дизайну

ОРГАНІЗАЦІЯ ЗАХИСТУ ОБЛІКОВОЇ ІНФОРМАЦІЇ В УМОВАХ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

У статті доведено важливість облікової інформації для господарського життя суб'єкта господарювання. Наведено приклади впливу кібератак на систему бухгалтерського обліку та пов'язаних із ними витрат. Окреслено ризики, з якими стикаються електронні бухгалтерські інформаційні системи на основі виділення ризиків для усіх складових процесу бухгалтерського обліку. Доведено, що захист облікової інформації та уникнення «гачка» кібератаки можливий лише у випадку дотримання комплексних заходів та спільних дій керівного персоналу, облікового персоналу, аудиторів та закладів освіти при навчанні майбутніх фахівців.

***Ключові слова**: облікова інформація, кібербезпека, кібератака, інформаційна безпека, ризик.*

Скрыпник Маргарита Ивановна,
доктор экономических наук, профессор, заведущая кафедри учета и аудиту Киевского национального университета технологий и дизайна

Григоревская Елена Александровна,
кандидат экономических наук, доцент, доцент кафедри учета и аудиту Киевского национального университета технологий и дизайна

ОРГАНИЗАЦИЯ ЗАЩИТЫ УЧЕТНОЙ ИНФОРМАЦИИ В УСЛОВИЯХ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

В статье доказана важность учетной информации для хозяйственной жизни предприятия. Приведены примеры влияния кибератак на систему бухгалтерского учета и связанных с ними расходов. Определены риски, с которыми сталкиваются электронные бухгалтерские информационные системы на основе выделения рисков для всех составляющих процесса бухгалтерского учета. Доказано, что защита учетной-информации и избежания «крючка» кибератаки возможен лишь в случае соблюдения комплексных мероприятий и совместных действий руководящего персонала, учетного персонала, аудиторов и учреждений образования при обучении будущих специалистов.

***Ключевые слова:** учетная информация, кибербезопасность, кибератака, информационная безопасность, риск.*

Margarita Skrypnyk,
Doctor of Economics, Professor, Head of the Department of Accounting and Auditing Kyiv National University of Technology and Design

Olena Hryhorevska,
PhD, Associate Professor, Associate Professor of Accounting and Auditing Kyiv National University of Technology and Design

ORGANIZATION OF ACCOUNTING INFORMATION PROTECTION IN TERMS OF CYBER SECURITY

The purpose of the article is to summarize the existing approaches and outline promising areas for the organization of protection of accounting information in terms of cybersecurity. In the course of the research methods of observation, comparison, analysis, synthesis, generalization were used. The article proves the importance of accounting information for the economic life of the business entity. The importance of the Internet and IT technologies application to reflect certain facts of economic life in the accounting system (cash flow management, sales process, calculations, delivery, online trade, reporting)is substantiated. As shown in the example of the impact of cyberattacks on the accounting system and related costs are described on the example of the Program-Fraudster Violation of confidentiality Hacking Malicious software. The risks faced by electronic accounting information systems based on the allocation of risks for each component of the accounting process (risks associated with the collection and input of data into an automated system; risks associated with information processing and storage on electronic media; risks associated with stage of generalization and transfer of information). It is proved that the protection of accounting information and avoidance of the «hook» of a cyber attack is possible only in the case of compliance with comprehensive measures and joint actions of management, accounting staff, auditors and educational institutions in the training of future professionals. It is concluded that effective communication and strategies between management, accountants and auditors are important to reduce or protect against emerging threats to the accounting information system.

***Key words**: accounting information, cybersecurity, cyberattack, information security, risk.*

Постановка проблеми. У Звіті «COVID-19: карта ризиків і наслідків» (COVID-19 Risks Outlook), опублікованого Всесвітнім економічним форумом, розкрито вже відомі ризики, які можуть бути максимізовані пандемією, і нові, які вона тільки продукуватиме. У звіті використані результати опитування майже 350 топ-менеджерів і фахівців з оцінки ризиків. Від них вимагалось окреслити найважливіші проблеми, які можуть виникнути, як для всього світу, так і для їх бізнесу. Так, п'ятірка ризиків та загроз-лідерів, на думку респондентів, протягом наступних 18 місяців виглядатиме так: тривалий спад світової економіки (66,3 %); сплеск банкрутств і посилення консолідації галузей (52,7 %); кібератаки і шахрайство з даними через віддалені роботи (50,1 %); нездатність деяких галузей і секторів повністю відновитися (50,1 %); затяжні збої глобальних ланцюжків постачань (48,4 %) [2].

Отже, зауважимо, що технології зіграли ключову роль в тому, як суспільство, підприємства та уряди мінімізують наслідки кризи COVID-19. А «безконтактна» економіка також може створити нові можливості працевлаштування в постпандемійному світі. Однак велика залежність від технологій збільшила ризики кібербезпеки. На думку 38 % опитаних експертів, нові робочі схеми (наприклад, віддалена робота) призводять до кібератак і шахрайства з даними та продукують найбільш ймовірний ризик технологічних наслідків для всього світу. Швидке поширення нових технологічних рішень загострило інші ризики, такі як цифрова фрагментація, порушення конфіденційності і нерівність. Таким чином, COVID-19 може кинути виклик взаємозв'язку між технологіями та управлінням, в той час як недовіра або неправильне використання технологій можуть мати довгострокові наслідки для суспільства [12].

Інформаційна захищеність є одним з найважливіших аспектів загальної безпеки на різних рівнях – національному, галузевому, корпоративному, персональному. Це пов'язано з тим, що в сучасному світі експонентний приріст кількості інформації перетворив її з другорядного ресурсу в чинник, який вирішальним чином впливає практично на всі сфери суспільного життя, відображаючи тим самим зростаючу інформаційну залежність суспільства [3].

В свою чергу, інформаційна система бухгалтерського обліку формується з конфіденційної та приватної інформації, яка може бути порушена, якщо її не захистити. Несанкціоноване використання інформації, сформованої в системі бухгалтерського обліку, може призвести до згубних наслідків, ризикуючи втратою інформації, неправильним введенням даних та зловживанням конфіденційною інформацією [9]. Неадекватна інформаційна безпека збільшує можливість маніпулювання, фальсифікації або зміни бухгалтерських записів [11]. Тому питання захисту інформації, сформованої в системі бухгалтерського обліку, є надзвичайно актуальними, а забезпечення її безпеки є пріоритетом у багатьох фірмах.

Аналіз останніх досліджень та публікацій. Питанням, присвяченим проблемним аспектам визначення загроз порушення балансу кібер- та інформаційної безпеки, присвячено дослідження І. Л. Грабчук, О. О. Конопліна, Ю. М. Попівняк, И. В. Федоренко, П. Харламов, Н. О. Чех, Д. С. Шахвердян [8] та інших науковців та практиків. Дослідження наведених авторів справді цікаві та висвітлюють особистий підхід до збереження бухгалтерської інформації, розробки заходів до підвищення її захищеності та попередження порушення інформаційної безпеки та кібератак. Проте підходи до організації захисту інформації в умовах забезпечення кібербезпеки потребують додаткового узагальнення. Актуальним є окреслення внеску кожного причетного до провадження господарської діяльності підприємства у формування засобів та напрямів захисту інформації та огляд сучасних підходів управління досліджуваною предметною областю.

Мета і завдання дослідження: узагальнити існуючі підходи та окреслити перспективні напрями до організації захисту облікової інформації в умовах забезпечення кібербезпеки.

Виклад основного матеріалу. Як зауважує Ю. Попівняк, «інформація про факти господарського життя підприємства формуються в системі бухгалтерського обліку та характеризується високим ступенем цінності. Вона є запорукою стійкості, розвитку та ефективності діяльності такого підприємства, але лише за умови її надійного захисту» [5]. Несанкціонований або невідповідний доступ до інформаційної системи бухгалтерського обліку або нездатність встановити і підтримувати поділ обов'язків в рамках системи внутрішнього контролю може ускладнити забезпечення реєстрації, обробки та подання достовірних і точних транзакцій. Активне застосування інтернет- та ІТ-технологій системою бухгалтерського обліку (на прикладі окремих операцій), які можуть зазнати впливу ризику кібератаки можемо навести у табл. 1.

Таблиця 1

Застосування Інтернет- та ІТ-технологій при відображенні окремих фактів господарського життя в системі бухгалтерського обліку

Господарська операція	Характеристика
Управління грошовими потоками	Інформаційна система бухгалтерського обліку забезпечує процес управління, який включає в себе дані про грошові кошти, запаси і реалізацію. Комп'ютеризована система може надати інформацію набагато швидше, ніж неавтоматизований облік, що робить її важливим інструментом в управлінні готівкою і рівнем запасів
Процес реалізації	Визнання процесу реалізації – це перший крок до формування виручки. Система бухгалтерського обліку визнає реалізацію як збільшення виручки разом зі збільшенням грошових коштів або дебіторською заборгованістю. На підприємствах роздрібної торгівлі також необхідно зменшити запаси – цей тип транзакції автоматично обробляється за допомогою комп'ютеризованої системи. Багато фірм впроваджують програмне забезпечення для торгових точок, яке дозволяє сканувати товари і передавати дані в систему бухгалтерського обліку в режимі реального часу, що є основною перевагою в управлінні грошовими коштами і запасами
Розрахунки	Платежі, за якими уважно стежить керівництво, збільшують грошові потоки. Залежно від типу бізнесу платежі можуть здійснюватися у формі чеків, кредитних карт, готівки, банківського переказу та грошових переказів. Ці транзакції фіксуються в системі бухгалтерського обліку за допомогою записів заповнюється вручну журналу або інтерфейсів з інших систем. У деяких компаній є спеціальні модулі дебіторської заборгованості, які розпізнають не тільки дані бухгалтерського обліку, але також деталі продажів, умови, контакти та іншу інформацію. Коли платіж отриманий, бухгалтер вводить свої платіжні реквізити в модуль, яка надходить в головну книгу
Доставка	Доставка – життєво важлива частина циклу доходів. В інтегрованих системах доставки діяльність відображається в головній книзі, в основному у частині інвентаризації. Система реєструє всі відповідні транзакції, тому співробітникам, які працюють на складі, не потрібно знати бухгалтерський облік для правильного виконання цієї діяльності. Функція відвантаження складається з двох частин: відбір товару і відвантаження. Штрих-коди часто використовуються для прискорення цього процесу, документування та зменшення інвентарних рахунків.
Інтернет-торгівля	Інтернет усунув фізичні бар'єри для торгівлі, відкривши доступ до раніше нерентабельних ринків. Можливості інтернету в полегшенні ведення бізнесу можуть бути серйозно нівельовані турботою користувачів про безпеку. Проблеми з веб-сайтом, з якими іноді стикаються великі постачальники послуг електронної комерції, як-от: Yahoo, eBay, E-Trade і Amazon.com – свідчать про деякі ризики атак
Звітність	Інформаційна система бухгалтерського обліку може створювати звіти, які використовуються керівництвом для прийняття рішень з фінансових питань. Деякі загальні звіти – це звіти про рівень запасів, аналіз тенденцій і звіти про терміни погашення дебіторської заборгованості, які повідомляють менеджеру, хто є боржником, скільки вони винні і терміни оплати. Без комп'ютерної системи було б дуже складно складати ці докладні звіти своєчасно і ефективно

Джерело: систематизовано та доповнено на основі [14], [11].

За підрахунками інциденти з кібербезпекою загрожують деяким людям на десятки тисяч доларів. Кібератака, яка призводить до значного порушення даних, може мати згубні наслідки не тільки для операційної сторони фірми, але також матиме юридичні наслідки для директорів бізнесу, коли вищий менеджмент може зіткнутися з регуляторним розслідуванням або судовим розглядом.

Порушення даних також може спричинити значний ризик довіри та репутації, що може призвести до втрати доходу / зниження ціни акцій публічно зареєстрованих компаній.

Як у своїх дослідженнях зауважує Карен Макдональд (Karen McDonald), «австралійці втратили мільйони доларів в 2019 р. через фішинг-електронні листи та текстові повідомлення, що видають себе за банки або постачальників комунальних послуг, які шукають дані для входу; фальшиві онлайн-вікторини, опитування та оголошення про роботу» [13]. А одне з останніх податкових шахрайств австралійського податкового управління націлене на жертв недавніх стихійних лих, обіцяючи 8 % бонусу на податкові

декларації 2020 р., якщо отримувач натисне посилання, яке переведе їх на підроблений веб-сайт myGov, призначений для викрадення особистої інформації, в тому числі імена, адреси, електронні листи, номери телефонів та банківські реквізити.

Таким чином, дослідження випадків кіберзлочинності та пов'язаних з нею витрат показує значне зростання. У табл. 2 наведено декілька прикладів випадків кіберзлочинності та пов'язаних із ними витрат, які часто є значними.

Таблиця 2

Приклади впливу кібератак на систему бухгалтерського обліку та пов'язаних із ними витрат (на прикладі аутсорсингових компаній Австралії)

Вид кібератаки, збіток	Опис ситуації
Программа-Шахрай Загальна вартість: 83660 дол. США	Невелика бухгалтерська фірма з 10 співробітниками зазнала атаки після того, як один із співробітників відкрив електронний лист, що, на його думку, містив вкладений рахунок-фактуру. В додатку містився вірус Cryptolocker. Всі комп'ютери в офісі припинили роботу, і з'явилося повідомлення з вимогою 8000 дол. (сплачується в біткойнах) за запуск системи. Сума збільшуватиметься ще на 1200 дол. на день до тих пір, поки не буде сплаченою. Витрати включали не лише оплату викупу, але й витрати на IT-криміналістику, відновлення системи після того, як було виявлено, що вона працює з помилками після її запуску, витрати від простою у діяльності, витрати на зв'язок з громадськістю, а також витрати на повідомлення контрагентам, з якими було порушено зв'язок
Порушення конфіденційності. Загальна вартість: 246000 дол. США плюс постійні судові розгляди від осіб, особисті дані яких порушено	Працівник середньої бухгалтерської фірми випадково залишив флешку USB, що містить особисті дані кількох клієнтів, у таксі. Виявивши збиток, працівник повідомив своїх роботодавців, які залучили спеціалізовані установи для виявлення клієнтів, чиї персональні дані були викриті. Постраждало 175 клієнтів, про що їх слід було повідомити. Крім того, дані про усіх постраждалих зберігались протягом наступних 12 місяців у Службі кредитного моніторингу та PR-компанії, найнятої для відновлення довіри та пом'якшення негативної реклами, спричиненої подією
Злом. Загальна вартість, включаючи пов'язане з цим переривання бізнесу: 330000 дол. США	Незадоволений співробітник фірми з фінансових послуг змінює всі паролі адміністратора до мережі, що фактично відключило усю компанію від системи. Доступ до системи довелося відновлювати. У цей час фірма не могла працювати
Зловмисне програмне забезпечення. Загальна вартість: 300000 дол.	Комп'ютерна система хмарного постачальника бухгалтерської фірми відключена внаслідок агресивного комп'ютерного вірусу. Крім того, бізнес зазнає втрат прибутку під час відновлення системи та протягом 6 місяців після
Крадіжки особистих даних. Загальна вартість 140000 дол. США	Бухгалтерська фірма зазнала злому, а на кількох ноутбуках було викрадено інформацію про клієнтів та персонал. На жаль, цю інформацію не було зашифровано. Кілька клієнтів стали жертвами викрадення особистих даних, в результаті чого подали позов за збитки. Крім того, фірма понесла значні витрати на повідомлення всіх постраждалих клієнтів/співробітників та надання послуг кредитного моніторингу протягом двох років
Соціальна інженерія. Загальна вартість 174000 дол. США	Пізно ввечері в п'ятницю перед вихідними (державне свято) старший співробітник бухгалтерської фірми отримав електронного листа нібито від клієнта з повідомленням про зміну реквізитів банківського рахунку цього клієнта і з проханням перенаправити терміновий платіж на новий рахунок. Лист виглядав справжнім, і співробітник перерахував гроші. Через 2 тижні клієнт зв'язався для оплати, і співробітники повідомили їм, що оплату було проведено. В результаті розслідування було встановлено, що злом мережі стався 6 тижнями раніше

Джерело: систематизовано на основі [13].

Таким чином, існує ряд загроз для інформаційних систем бухгалтерського обліку, особливо для тих систем, які використовуються спільно з інтернетом. Ці загрози є проблемами для менеджменту, бухгалтерів, аудиторів і вчених.

Щодо виділення ризиків загрози безпеці бухгалтерських даних, то дослідниками виділяється цьому питанню достатньо уваги.

Так, Ю. М. Повівняк акцентує увагу на «застосуванні слабких інструментів аутентифікації користувачів бухгалтерської інформації; нехтуванні правилами захисту робочих комп'ютерів чи інших пристроїв, з яких відбуваються доступ і робота з обліковими даними; застосуванні робочих пристроїв у неробочих цілях; браці у бухгалтерів елементарних знань з основ кібербезпеки; неправильній розстановці пріоритетів і відсутності належної підтримки з боку системи менеджменту підприємства; нехтуванні правилами збереження бухгалтерських даних і їх періодичного резервування; ігноруванні наявних ризиків і негативного досвіду інших учасників ринку; відсутності на підприємстві відповідного спеціаліста із захисту бухгалтерської інформації тощо» [5].

І. Л. Грабчук зауважує, що «одним із найпоширеніших видів інформаційних загроз з використанням інформаційно-комп'ютерних технологій є вірусні атаки, що пошкоджують не тільки програмне забезпечення комп'ютерів, але і призводять до їх поламок та несправностей» [4].

І. В. Федоренко зазначає, що «специфічною загрозою інформаційній безпеці облікової інформації є недостовірність інформації, яка може виникнути внаслідок впливу ряду факторів, зокрема, через помилки у використовуваному програмному забезпеченні» [6].

Ш. Шенкер (Sheila Shanker) у своєму дослідженні наводить перелік ризиків, пов'язаних з системами бухгалтерського обліку, – від бронювання фальшивих транзакцій до крадіжки резервної стрічки зі всією фінансовою інформацією. Приклади ризиків: крадіжка номерів соціального страхування у співробітників і підрядників; платежі підробленими постачальникам; видалення/втрата даних; пошкодження резервних стрічок; крадіжка серверів або комп'ютерів [14].

Проте, цікавим підходом, з яким варто погодитись, є підхід до виділення груп ризиків, запропонований А. Абдуллахом (Ayedh Abdullah), який навів ризики, виходячи із процесів, що включає у себе бухгалтерський облік: процесу збору, накопичення, систематизації, узагальнення облікової інформації (табл. 3).

Таблиця 3

Ризики, із якими стикаються електронні бухгалтерські інформаційні системи

Ризик	Зміст	Характекристика
Ризики, пов'язані зі збором та введенням даних в автоматизовану систему	1. Персонал неправильно вводить (ненавмисно/навмисно) дані. 2. Ненавмисне знищення даних співробітниками. 3. Умисне знищення даних співробітниками	Маскування (удавання авторизованого користувача) і поєднання (підключення до телекомунікаційних лініях) є прикладами хакерських дій, які можуть серйозно вплинути на збір достовірних даних
Ризики, пов'язані з обробкою інформації та її зберіганням на електронних носіях	1. Незаконний доступ (несанкціонований) до даних і системи співробітниками. 2. Незаконний доступ до даних і системи з боку людей ззовні. 3. Участь багатьох співробітників в одному паролі. 4. Впровадження комп'ютерного вірусу для облікової системи та вплив на роботу системи даних. 5. Перехоплення і доступ до даних з серверів на комп'ютери користувачів	Незаконний доступ до файлів або їх видалення, знищення або пошкодження логіки програми за допомогою вірусів або зміна логіки програми, що змушує додаток обробляти дані неправильно. Нездатність підтримувати файли резервних копій або інші методи вилучення зумовлює потенційно руйнівну втрату даних
Ризики, пов'язані з етапом узагальнення та передачею інформації	1. Знищення. 2. Формування фальсифікованої звітності. 3. Крадіжка даних/інформації. 4. Копіювання 5. Несанкціоноване розкриття даних шляхом відображення на екрані або друку на папері. 6. Роздруківка і поширення інформації сторонніми особами 7. Передача конфіденційних документів людям, що не відповідає вимогам безпеки, для їх розриву або утилізації	Крадіжка, перенаправлення або неправильне використання комп'ютерних даних може завдати шкоди конкурентоспроможності або репутації організації

Джерело: узагальнено та доповнено на основі [10].

Так, об'єктивно, що наявність виділених загроз продукує розробку методів їх мінімізації. Так, зокрема, Д. Берд та Дж. Вен (Deborah Beard, H. Joseph Wen), наголошуючи на необхідності захисту від ризиків, зауважують, що у випадку їх ігнорування, вони можуть підірвати актуальність і надійність фінансової інформації, що призведе до прийняття неправильних рішень різними зацікавленими сторонами [11].

І. Л. Грабчук пропонує заходи для мінімізації ризиків в частині логічної (ідентифікація ризиків, розгляд забезпечення інформаційної безпеки підприємства як частини корпоративної культури) та фізичної (шифрування даних, фізичний захист технічного забезпечення) безпеки. Врахування цих заходів дозволить значно мінімізувати наслідки кібератак [4].

Ш. Шенклер (Sheila Shanker) також ідентифікує дві групи методів управління ними: превентивні (з метою попередження ризиків) та детективні (з метою виявлення проблем посфактум). Як тільки ризики ідентифіковані, можна налаштувати засоби управління для захисту системи: часта зміна пароля; шифрування даних; щомісячна перевірка звітів постачальників; безпечне і захищене серверне і комп'ютерне середовище; безпечне і захищене архівування резервних стрічок поза офісом [14].

С. А. Вітер та І. І. Світлишин виділяють три групи заходів: 1) організаційні (обмеження несанкціонованого доступу до конфіденційної облікової інформації); 2) технічні (попередження навмисного пошкодження облікової інформації за допомогою спеціально спровокованих порушень працездатності технічних засобів або програмного забезпечення); 3) кадрова робота (підвищення компетентності працівників та їх відповідальності у застосуванні новітніх інформаційних технологій) [1].

Можемо погодитись з усіма вищенаведеними пропозиціями. Адже кожен суб'єкт господарювання намагається уникнути ризиків кібератак та забезпечити інформаційну безпеку інформації будь-яким способом.

Але, на нашу думку, захист облікової-інформації та уникнення «гачка» кібератаки можливий лише у випадку дотримання комплексних заходів та спільних дій керівного персоналу, облікового персоналу, аудиторів та, як не дивно, закладів освіти при навчанні майбутніх фахівців.

Так, наприклад, *керівник* підприємства повинен володіти такими знаннями та компетенцією, щоб розуміти порядок документування та вміти протестувати систему внутрішнього контролю. Це не означає, що керівник повинен бути бухгалтером за фахом або бути фахівцем у сфері програмування чи захисту інформації. Але керівник повинен розуміти сутність усіх операцій та цікавитись такими питаннями, як реальна наявність активів та зобов'язань вказаних у фінансовій звітності; дійсність відображення зареєстрованих та відображених у звітності господарських операцій та чи усі операції відображено; чи правильно класифікуються та розкриваються об'єкти бухгалтерського обліку у фінансовій звітності; чи можна довіряти відповідям відповідальних працівників, якщо існує загроза інформаційній безпеці підприємства, а керівництво не вжило заходів для захисту організації від внутрішніх та зовнішніх загроз?

Бухгалтери повинні бути інформовані про загрози безпеки і відповідних методах контролю, щоб захистити свої інформаційні системи і консультувати підприємства щодо ризиків безпеки. Важливим є забезпечення бухгалтерів встановленими найсучаснішими антивірусними програмами. Актуальним є вміння розпізнавати шахрайство по електронній пошті, що не адресована напряму. Наприклад, К. Макдональд (Karen McDonald) наводить 6 способів розпізнання фальшивих листів: низький рівень граматики/орфографії, неякісні ілюстрації; наявність інструкції переходу за посиланням; дивне походження; відчуття терміновості [13]. Крім того, важливо якчастіше створювати резервні копії даних та використовувати складні паролі. І, звичайно, уникати відкриття вкладень від невідомих осіб у листі.

Важливим суб'єктом забезпечення уникнення загроз кібератак підприємства є *аудитор* (зовнішній, внутрішній). Так, процедури, коли аудитор може призначити ІТ-фахівця, включають: з'ясування того, які дані і транзакції ініціюються, реєструються, обробляються і визнаються; які впроваджено засоби управління ІТ; перевірка системної документації; спостереження за роботою засобів контролю ІТ; планування і виконання тестів ІТ-засобів управління. Аудитор повинен мати достатні знання в області ІТ, щоб довести до відома ІТ-фахівця мету аудиту, оцінити, чи будуть процедури відповідати цілям аудитора, а також оцінити результати процедур, оскільки вони пов'язані з характером, термінами і обсягом інших аудиторських процедур [11].

Науковці і викладачі. В сучасних реаліях важливим аспектом підготовки майбутніх фахівців є розуміння ними необхідності ІТ-безпеки і важливість спільної роботи з іншими над розробкою політик, процесів і технологій для усунення загроз. Сьогодні від майбутніх фахівців з обліку і оподаткування слід вимагати знання, навички та етику, які дозволять їм розуміти бізнес-середовище, проводити оцінку ризиків, оцінювати внутрішній контроль та впроваджувати ефективні і дієві заходи безпеки. Важливо прагнути до інтеграції тим і методів безпеки в навчальні програми з бухгалтерського обліку.

Як зауважують Д. Берд та Д. Вен (Deborah Beard, H. Joseph Wen), сертифікати CPA (підтверджує професійні знання у галузі аудиту, господарського права, фінансового обліку та звітності, оподаткування), CMA (Сертифікований бухгалтер з управлінського обліку) і CIA (дипломований внутрішній аудитор) все більше визнають важливість ІТ. На іспиті CPA від 12 % до 18 % в розділі «Аудит і атестація» і від 22 % до 28 % в тестових темах розділу «Бізнес-середовище та концепції» відносяться до комп'ютеризованої середовищі і її впливу на ІТ в бізнес-середовищі. На іспиті CMA 15 % частин I і II враховуються при визначенні очікуваних ризиків, внутрішнього контролю, системного контролю та безпеки, розробки і проектування систем, електронної комерції, систем планування ресурсів підприємства (ERP) і іншим областям, пов'язаних з інформаційними системами і технологіями. На іспиті CIA від 30 % до 40 % частини III охоплює ІТ, включаючи структури управління, дані і мережевий зв'язок, електронний обмін даними, шифрування і захист інформації [11].

Нові професійні позначення, такі як сертифікований фахівець з інформаційних технологій (CITP), сертифікований аудитор інформаційних систем (CISA) і сертифікований фахівець з безпеки інформаційних систем (CISSP) – демонструють потребу в сертифікації, пов'язаної з інформаційними технологіями, системним аудитом і безпекою систем.

Ще одним перспективним напрямом мінімізації ризиків є комплексне кіберстрахування. Так, це явище є новим як для світового ринку страхових послуг, так і українського, де покривається лише 5 % страхових випадків кібератак. Зауважимо, що на ринку страховиків такі послуги надають СК Рідна, СК Інго, СК Аска та інші. Як зауважує П. Харламов, «за даними Munich Re, подібний захист пропонують у цілому 60 страхових компаній у різних країнах. Водночас страхуванням покрито лише 5 % кібер-ризиків. Проте валоподібне зростання загроз із боку хакерів стимулює розвиток цього напрямку, і за оцінками тієї ж Munich Re, обсяги кібер-страхування у 2020 р. складуть вже 8–9 млрд дол. проти 3,4–4 млрд дол. у 2017 р. А

згідно з дослідженням страхової групи Allianz ринок кібер-страхування зростає на 25–50 % щороку» [7].

Отже, розуміння потреби в безпеці – спільний знаменник. Безпека електронної інформації стала критичною проблемою. Вчені, менеджери, бухгалтери і аудитори повинні бути інформовані про виникаючі загрози і заходи безпеки, які ефективні для забезпечення безпеки інформаційних систем бухгалтерського обліку.

Висновки. Таким чином, ефективна комунікація та стратегії між керівництвом, бухгалтерами та аудиторами важливі для зменшення або захисту від виникаючих загроз інформаційній системі бухгалтерського обліку. Щоб правильно оцінити потенційні ризики, бухгалтери та аудитори повинні бути знайомі з поточними і новими технологіями. Контроль несанкціонованого доступу до бухгалтерських записів є важливим компонентом внутрішнього контролю. Політика доступу і паролів, шифрування, цифрові підписи, блокування дисків, міжмережеві екрани і цифрові сертифікати є прикладами заходів контролю, які повинні бути ідентифіковані, задокументовані, повідомлені і піддані перевірці при оцінці ефективності контролю.

Література:

1. Вітер С.А., Світлишин С.А. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство: електронне фахове видання*. 2017. № 11. С. 497–502

Viter, S.A., Svitlyshyn, S.A. (2017) Zakhyst oblikovoi informatsii ta kiberbezpeka pidpryiemstva [Protection of accounting information and cybersecurity of the enterprise]. *Ekonomika i suspilstvo: elektronne fakhove vydannia* [Economy and society: electronic professional publication]. no 11. 497–502 (in Ukraine)

2. Влияние пандемии: обзор глобальных рисков URL: https://coronavirus.marsh.com/ru/ru/insights/research-and-briefings/covid-19-risks-outlook-preliminary-mapping-and-implications.html (дата звернення: 04 грудня 2020)

Vliyanie pandemii: obzor global'nyh riskovков [The impact of a pandemic: an overview of global risks] <https://coronavirus.marsh.com/ru/ru/insights/research-and-briefings/covid-19-risks-outlook-preliminary-mapping-and-implications.html> (04 December 2020). [in Russian].

3. Глухов Н.И. Оценка информационных рисков предприятия: учебное пособие. Иркутск : ИрГУПС, 2013. 148 с.

Gluhov, N.I. (2013). Ocenka informacionnyh riskov predpriyatiya: uchebnoe posobie [Enterprise Information Risk Assessment]. Irkutsk: IrGUPS, 148. [in Russian].

4. Грабчук І.Л. Організація захисту облікової інформації в умовах гібридної війни. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналіз*. 2018. № 3(41). С. 20-24.

Hrabchuk, I.L. (2018) Orhanizatsiia zakhystu oblikovoi informatsii v umovakh hibrydnoi viiny. [Organizing the search for regional information in the minds of the hybrid]. *Problemy teorii ta metodolohii bukhhalterskoho obliku, kontroliu i analiz.* [Problems of the theory and methodology of the accounting department, control and analysis]. no 3(41). 20-24. [in Ukraine].

5. Попівняк Ю.М. Кібербезпека та захист бухгалтерських даних в умовах застосування новітніх інформаційних технологій. *БІЗНЕС-ІНФОРМ* № 8 2019 С. 150-157.

Popivniak, Yu.M. (2019). Kiberbezpeka ta zakhyst bukhhalterskykh danykh v umovakh zastosuvannia novitnikh informatsiinykh tekhnolohii. [Cybersecurity and protection of accounting data in the application of the latest information technologies]. *BIZNES-INFORM* [BUSINESS INFORM]. no. 8. 150-157. [in Ukraine].

6. Федоренко И.В. Методические вопросы оценки риска информационной безопасности в бухгалтерском учете. *Вестник Крас ГАУ*. 2015 № 3 С. 161-168.

Fedorenko, I.V. (2015). Metodicheskie voprosy ocenki riska informacionnoj bezopasnosti v buhgalterskom uchete. [Methodological issues of information security risk assessment in accounting]. *Vestnik Kras GAU.* [Kras GAU Bulletin]. no 3. 161-168. [in Russian].

7. Харламов П. Пігулка від хакерів: як бізнес захищає себе від кібератак. URL: https://mind.ua/publications/20192978-pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak (дата звернення: 04 грудня 2020)

Kharlamov, P. Pihulka vid khakeriv: yak biznes zakhyshchaie sebe vid kiberatak [Pill from hackers: how business protects itself from cyberattacks]. <https://mind.ua/publications/20192978-pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak> (04 December 2020). [in Ukraine].

8. Чех Н.О., Конопліна О.О, Шахвердян Д.С. Забезпечення інформаційної безпеки бухгалтерського обліку підприємства. *Комунальне господарство міст. Серія : Економічні науки*. 2019. Вип. 2. С. 111-117.

Chekh, N.O., Konoplina, O.O, Shakhverdian, D.S. (2019). Zabezpechennia informatsiinoi bezpeky bukhhalterskoho obliku pidpryiemstva [Ensuring information security of accounting of the enterprise]. *Komunalne hospodarstvo mist. Seriia : Ekonomichni nauky* [Municipal utilities. Series: Economic Sciences]. no. 2. 111-117. [in Ukraine].

9. Accounting Information Systems Security Issues Sheila Shanker September 26, 2017 URL: https://bizfluent.com/list-6396287-accounting-information-systems-security-issues.html (дата звернення: 04 грудня 2020).

Accounting Information Systems Security Issues Sheila Shanker September 26, 2017 <https://bizfluent.com/list-6396287-accounting-information-systems-security-issues.html> (04 December 2020). [in English].

10. Ayedh Abdullah. Risk of computerizing accounting information systems in the libyan bank. *South East Asia Journal of Contemporary Business, Economics and Law*, 2018. Vol. 10, Issue 1 p.74-79

Ayedh, Abdullah. (2018). Risk of computerizing accounting information systems in the libyan bank. *South East Asia Journal of Contemporary Business, Economics and Law*, Vol. 10, Issue 1. 4-79 [in English.

11. Deborah Beard, H. Joseph Wen. Reducing the Threat Levels for Accounting Information Systems. *Challenges for Management, Accountants, Auditors, and Academicians The CPA Journal*. 2017 URL: http://archives.cpajournal.com/2007/507/essentials/p34.htm (дата звернення: 04 грудня 2020).

Deborah, Beard, H. Joseph, Wen. (2017) Reducing the Threat Levels for Accounting Information Systems. *Challenges for Management, Accountants, Auditors, and Academicians The CPA Journal*. <URL: http://archives.cpajournal.com/2007/507/essentials/p34.htm> (04 December 2020). [in English].

12. Emilio Granados, Franco Richard Lukacs, Marie Sophie Müller. Philip Shetler-Jones, Saadia Zahidi. COVID-19 Risks Outlook. A Preliminary Mapping and Its Implications May 2020. URL: https://go.pardot.com/l/395202/2020-05-19/bm4tdn/395202/206461/covid19_risks_outlook_en_uk.pdf (дата звернення: 04 грудня 2020).

Emilio Granados, Franco Richard Lukacs, Marie Sophie Müller, Philip Shetler-Jones, Saadia Zahidi. (2020). COVID-19 Risks Outlook. A Preliminary Mapping and Its Implications May 2020. <https://go.pardot.com/l/395202/2020-05-19/bm4tdn/395202/206461/covid19_risks_outlook_en_uk.pdf> (04 December 2020). [in English].

13. Karen McDonald. Cyber crime – The threat is real and could dramatically affect you and your accounting firm 2020 URL: https://www.accountancyinsurance.com.au/cyber-crime-threat/ (дата звернення: 04 грудня 2020).

Karen McDonald. Cyber crime – The threat is real and could dramatically affect you and your accounting firm 2020 <https://www.accountancyinsurance.com.au/cyber-crime-threat/>. (04 December 2020). [in English].

14. Sheila Shanker. The Revenue Cycle in Accounting Information Systems 2017. URL: https://bizfluent.com/info-8001409-revenue-cycle-accounting-information-systems.html (дата звернення: 04 грудня 2020).

Sheila Shanker. The Revenue Cycle in Accounting Information Systems 2017. <https://bizfluent.com/info-8001409-revenue-cycle-accounting-information-systems.html> (04 December 2020). [in English].