2. Вірус WannaCry пошкодив комп'ютери у 99 країнах світу. (2017, травень 13). *Головне.* BBC News Україна, Отримано травень 20, 2025, https://www.bbc.com/ ukrainian/features-39907984

3. Програми-вимагачі: вектор атак на підприємства. (2025). *Підтримка*. Eset, Отримано травень 20, 2025, https://www.eset.com/ua/support/information/ entsy klopediya-zahroz/ataka-prohram-vymahachiv-na-pidpryyemstvo/

4. Грищенко В. (2025, січень 14). Chainalysis придбав ШІ-платформу з виявлення шахрайства. *Бізнес*. Bitcoin Magazine, Отримано травень 20, 2025, https://bit coinmagazine.ua/technologies/1734956506-adam-bek-peven-shcho-kvantovi-obchi slen nya

Валькова Н.В.,
к.е.н., доцент,
Хмельницький національний університет

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБЛІКОВОЇ ІНФОРМАЦІЇ

У сучасних умовах функціонування економіки, що характеризуються високим рівнем цифровізації, поширенням кіберзагроз та загостренням конкурентної боротьби, безпека облікової інформації підприємств набуває критичного значення. Облікова інформація є основою для формування управлінської, фінансової, податкової, статистичної звітності, а також звітності зі сталого розвитку. Усі перелічені види звітності є інформаційною основою для аналітичного забезпечення прийняття управлінських рішень економічних систем різного рівня. Крім того, облікова інформація має виключне значення для здійснення контролю за діяльністю підприємств та забезпечення їх фінансової прозорості. Саме від її достовірності, повноти, своєчасності та захищеності залежить не лише ефективність управління, а й фінансова стабільність та репутація суб’єкта господарювання.

Особливо актуальним питання безпеки облікових даних стає в умовах війни, що проявляється у вигляді кібератак, порушень у ланцюгах постачання, перебоїв у роботі комунікацій та технічної інфраструктури. Підвищений ризик витоку конфіденційної інформації, її фальсифікації або знищення вимагає від підприємств застосування комплексних заходів захисту на всіх етапах облікового процесу. Крім того, впровадження хмарних сервісів, онлайн-доступу до облікових систем і дистанційної роботи додають вразливості обліковим системам та спричиняють потребу негайного реагування на виклики та загрози, які виникають в сфері забезпечення їх безпеки.

Водночас зростає тиск з боку регуляторних органів щодо дотримання стандартів захисту персональних даних та фінансової звітності, що також обумовлює необхідність впровадження відповідних політик безпеки. Закон України «Про інформацію» [1] визначає правові основи інформаційних відносин та зобов’язує захищати інформацію, яка є власністю юридичних осіб. Облікові дані часто містять персональну інформацію фізичних осіб: працівників підприємства, власників, клієнтів, постачальників інших учасників господарських процесів (особисті дані працівників, в тому числі фінансові), отже, їх обробка потребує особливого рівня захисту, який регулюється Законом України «Про захист персональних даних» [2]. Закон України «Про бухгалтерський облік та фінансову звітність» [3] зобов’язує підприємства забезпечити збереження первинних документів, регістрів та звітності. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [4] передбачає вимоги до кіберзахисту в комп’ютерних системах, у тому числі тих, де обробляється облікова інформація. Також питання забезпечення кібербезпеки регулюються такими законодавчими актами як: Закон України «Про основні засади забезпечення кібербезпеки України» [5]; Закон України «Про ратифікацію Конвенції про кіберзлочинність» [6]; «Стратегія кібербезпеки України» (рішення РНБО України) [7]; «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» (рішення РНБО України) [8]; Постанова КМУ «Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури» [9].

Дедалі частіше використовуються підприємствами для сертифікації внутрішньої системи управління інформаційною безпекою міжнародні стандарти (наприклад ISO/IEC 27001 [10]).

Основні проблеми, пов’язані із забезпеченням безпеки облікової інформації можна поділити на наступні: зовнішні кіберзагрози; проблеми низького рівня інформаційної культури; проблеми технічного захисту; проблеми, які виникають через недотримання законодавчих вимог; проблеми піратського програмного забезпечення; проблеми, викликані війною.

До зовнішніх кіберзагроз можемо віднести хакерські атаки (віруси, фішинг, DDoS), використання хмарних сервісів, може бути вразливим через неналежну політику безпеки провайдерів. Низький рівень внутрішньої інформаційної культури полягає у не дотриманні працівниками політик інформаційної гігієни (слабкі паролі, відкриті доступи, використання особистих пристроїв) та неналежна увага з боку роботодавця до освітніх заходів (тренінгів) з кібербезпеки для облікових працівників. Недосконаліть технічного захисту полягає у відсутності або використання застарілих антивірусних програм, систем резервного копіювання, поганому налаштуванні систем доступу до бухгалтерських та управлінських програм. Недотримання законодавчих вимог виникає через недостатній контроль за виконанням норм Законів України та застосування нестандартизованих процедур зберігання і передачі облікової інформації. Використання несертифікованого або піратського програмного забезпечення, яке може містити шпигунське програмне забезпечення або інші шкідливі елементи та відсутність регулярного оновлення ліцензійного програмного забезпечення також знижує рівень захисту системи. Ризиками під час воєнного стану або через надзвичайних ситуацій є: перебої з електропостачанням, доступом до інтернету або пошкодження серверів, зростання шпигунських і диверсійних кібератак, спрямованих на фінансові та адміністративні системи. Всі ці фактори можуть стати причинами несанкціонованого доступу до облікових даних, призвести до їх втрати або крадіжки.

Проблеми забезпечення безпеки облікової інформації так чи інакше пов’язані з інформаційним середовищем, в якому здійснюється обмін цією інформаціїєю, її накопичення, обробка, аналіз зберігання, а тому попри різноманітні причини виникнення тих чи інших загроз, вони всі матимуть характер кіберзагроз. Основними напрями вирішення цих проблем є: впровадження систем інформаційної безпеки відповідно до ISO/IEC 27001, забезпечення належного резервного копіювання облікових даних (автоматичне та регулярне), розмежування прав доступу до облікової інформації, здійснення аудиту інформаційної безпеки, забезпечення навчання персоналу з питань інформаційної етики та кібербезпеки. Таким чином, забезпечення безпеки облікової інформації є не лише технічним або юридичним завданням, а стратегічною умовою сталого розвитку підприємства, його конкурентоспроможності та здатності ефективно функціонувати в умовах змінного і ризикованого зовнішнього середовища.

Список використаних джерел

1. Верховна Рада України. (1992). *Закон України «Про інформацію» № 2657-XII від 02.10.1992*. https://zakon.rada.gov.ua/laws/show/2657-12#Text

2. Верховна Рада України. (2010). *Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010*. https://zakon.rada.gov.ua/laws/show/2297-17#Text

3. Верховна Рада України. (1999). *Закон України «Про бухгалтерський облік та фінансову звітність» № 996-XIV від 16.07.1999*. https://zakon.rada.gov.ua/laws/show/996-14#Text

4. Верховна Рада України. (1994). *Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 05.07.1994*. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

5. Верховна Рада України. (2017). *Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017*. https://zakon.rada.gov.ua/laws/show/2163-19#Text

6. Верховна Рада України. (2005). *Закон України «Про ратифікацію Конвенції про кіберзлочинність» № 2824-IV від 07.09.2005*. https://zakon.rada.gov.ua/laws/show/2824-15#Text

7. Президент України. (2021). *Указ № 447/2021 «Про Стратегію кібербезпеки України»*. https://zakon.rada.gov.ua/laws/show/447/2021#Text

8. Президент України. (2017). *Указ № 32/2017 «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»*. https://zakon.rada.gov.ua/laws/show/n0015525-16#Text

9. Кабінет Міністрів України. (2019). *Постанова № 518 від 19.06.2019 «Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури»*. https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

10. International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022)*. https://www.iso.org/standard/27001

Грабарєв А.В.,
кандидат економічних наук, доцент,
Мозговий С.А.,
здобувач третього (наукового) рівня вищої освіти,
Київський національний економічний університет імені Вадима Гетьмана

АНАЛІТИЧНІ ЗАСОБИ УПРАВЛІННЯ ПІДПРИЄМСТВОМ В КОНТЕКСТІ INDUSTRY 4.0

Анотація. У тезах досліджено трансформацію аналітичних засобів управління підприємствами під впливом концепції Industry 4.0. Розкрито етапи еволюції аналітики – від традиційних бухгалтерських і статистичних підходів до використання інтелектуальних систем, що працюють у режимі реального часу. Обґрунтовано значення прогнозних моделей, діагностичних алгоритмів, хмарної обробки даних та технологій інтернету речей (IoT) для реалізації цілісного підходу до управління в умовах цифрової трансформації. Здійснено