DOI: https://doi.org/10.35774/econa2024.03.403 **JEL classification: M41, M42, D24**
UDC: 657.6:008

Олег ШЕВЧУК
кандидат економічних наук, доцент,
доцент, кафедра обліку і оподаткування,
Західноукраїнський національний університет, Україна
E-mail: ikaf@ukr.net
ORCID iD: 0000-0002-7352-7001
https://www.webofscience.com/wos/author/record/H-3569-2017

ОРГАНІЗАЦІЯ ОБЛІКУ ТА КІБЕРБЕЗПЕКИ ЕЛЕКТРОННИХ ТРАНСАКЦІЙ ПІДПРИЄМСТВА

Анотація

Вступ. Цифровізація соціально-економічних процесів призвела до збільшення частки електронних трансакцій в грошових операціях. Електронні трансакції з використанням електронних та криптографічних валют є об'єктом підвищеної уваги зловмисників. Метою кібератак є не тільки заволодіння грошовими коштами, але й викрадення конфіденційної інформації, блокування інформаційних потоків, створення інформаційного хаосу, пошкодження програмно-технічного забезпечення та публічна дискредитація підприємства. Подолання варіативних кіберзагроз потребує організації ефективної системи кіберзахисту електронних трансакцій.

Мета. Мета статті полягає у ідентифікації кіберзагроз функціонуванню системи електронних трансакцій з пропозиціями щодо їх усунення через селекцію варіативних організаційних форм забезпечення кібербезпеки підприємства.

Результати. Інформаційною основою системи кібербезпеки підприємства запропоновано вважати бухгалтерський облік та контроль електронних трансакцій. Визначено напрямки ефективного кіберзахисту електронних трансакцій, які полягають у забезпеченні: конфіденційності, цілісності, доступності, порівнювальності та адресності облікової інформації про грошові операції. Для подолання кіберзагроз функціонуванню системи електронних трансакцій запропоновано використовувати технології: блокчейн, чат-ботів зі штучним інтелектом, біометрії, хмарних сервісів, моніторингу Інтернет-трафіку тощо.

Систематизовано організаційні варіанти кіберзахисту електронних трансакцій у напрямку: об'єднання розрізнених працівників у безпекові команди або створення окремого безпекового підрозділу підприємства; дистанційне залучення фахівців аутсорсера або періодичне їх прибуття до підприємства – замовника послуг аутсорсингу. Розроблено інформаційну схему дуального поєднання внутрішнього та зовнішнього безпекового контролю, що інтегрується в кластерний формат організації обліку електронних трансакцій. Доведено, що дуалізація контролю кібербезпеки забезпечує збалансування кіберризиків та витрат на організацію кіберзахисту електронних трансакцій. Такий формат організації кібербезпеки адаптивно актуальний для різних суб'єктів господарювання.

Врахування напрямків кіберзахисту, можливостей сучасних технологій у подоланні кіберризиків, функціональних повноважень безпекових працівників, а також організаційних форматів кібербезпеки грошових потоків забезпечує надійне функціонування системи електронних трансакцій на підприємстві. Забезпечення ефективного кіберзахисту в поєднанні з обліком і контролем електронних трансакцій є основною для організації комплексної системи кібербезпеки фінансово-господарської діяльності підприємства.

Отримано: 04.08.2024 р. **Рекомендовано до друку:** 03.09.2024 р. **Опубліковано:** 30.09.2024 р.

Як цитувати: Шевчук О. Організація обліку та кібербезпеки електронних трансакцій підприємства. *Економічний аналіз.* 2024. Том 34. № 3. С. 403-416. DOI: https://doi.org/10.35774/econa2024.03.403

Ключові слова: облік; кібербезпека; кіберризики; безпековий контроль; електронні трансакції; безпековий аутсорсинг.

Вступ

Грошові кошти незалежно від їх виду і форми завжди були об'єктом посягання зловмисників. Заволодіння чужими грошима, у тому числі електронними чи криптографічними валютами, є метою злочинних дій і дотепер. Цифровізація соціально-економічних процесів полегшила доступ до грошових розрахунків через електронні комунікації не тільки для учасників, але й для кіберзлочинців. Кіберзлочинці використовують специфічні методи та способи незаконного збагачення. В цьому злочинцям допомагає відкритість глобальної мережі та відсутність фізичного контакту з платниками чи одержувачами грошових коштів. Кіберзлочинці також використовують низьку обізнаність громадськості у функціонуванні системи електронних трансакцій. Для протидії злочинній діяльності у сфері електронних трансакцій активного розвитку набули системи кібербезпеки підприємств. Мета кіберзахисту електронних трансакцій полягає в обмеженні несанкціонованого доступу до грошових коштів та блокуванні грошових операцій.

Проте, кіберзлочини сьогодення націлені не тільки на привласнення грошових активів. Тотальна цифровізація соціально-економічних процесів призвела до активізації варіативних кіберзагроз. Оскільки система електронних трансакцій стає основою фінансово-господарської діяльності підприємств, зростає кількість кіберризиків, пов'язаних з грошовими потоками. До таких ризиків відносяться; втрата конфіденційної інформації, блокування інформаційних потоків, відмова програмно-технічного забезпечення, громадська дискредитація підприємства тощо. Подолання численних загроз функціонуванню системи електронних трансакцій потребує залучення обліково-контрольних фахівців як основних носіїв інформаційних атрибутів фінансово-господарської діяльності підприємств. Бухгалтерський облік і контроль електронних трансакцій доцільно позиціонувати основою організації кіберзахситу підприємства.

Взаємозв'язок бухгалтерського обліку і кібербезпеки підприємства є предметом наукових досліджень численних вітчизняних та зарубіжних вчених. Наприклад, Ю. Ю. Мороз та Ю. С. Цаль-Цалко сформували дефініційне позиціонування кіберзахисту облікової інформації «як захищеність життєво важливих інтересів підприємства від внутрішніх і зовнішніх загроз, його кадрового і інтелектуального потенціалу, комерційної таємниці, технологій, прибутку, доданої та ринкової вартості, інформація про які формується системою обліку і забезпечується сукупністю заходів спеціального правового, економічного, організаційного, інформаційно-технічного характеру» [1, с. 9]. Також В. М. Рожелюк визначає кіберзахист облікової системи «як сукупність дій облікових працівників з архівації даних, підтримки рівня професіоналізму облікових фахівців, організації ефективної системи комунікацій підприємства із стейкхолдерами, забезпечення належних умов праці бухгалтерів тощо» [2, с. 137]. С. А. Вітер та І. І. Світлишин сформували такі принципи кіберзахисту облікової підсистеми підприємства: «підтримка програмного забезпечення, охорона конфіденційної інформації, персональна відповідальність, секретність, комплексність, контроль доступу до облікових даних» [3, с. 501].

Якщо більшість науковців дотримуються спільної позиції щодо розуміння облікової природи кібербезпеки підприємства, дискусійним залишається вироблення заходів з подолання кіберризиків. Наприклад, В. А. Шпак виокремлює «чотири групи таких заходів: правові, технічні, програмні та організаційні» [4, с. 182–184]. С. М. Деньга та Ю. А. Верига визначають «активні і пасивні методики мінімізації загроз інформаційним системам обліку» [5, с.62]. І. Л. Грабчук пропонує «засоби логічної (розгляд забезпечення інформаційної безпеки підприємства як частини корпоративної культури) та фізичної безпеки (шифрування даних та фізичний захист технічного забезпечення) [6, с. 23]. Також, Ю. М. Попівняк ідентифікувала «організаційні, кадрові, технічні та юридичні кіберзагрози і розробила відповідні напрямками їх усунення з використанням інформаційних технологій» [7, с. 156].

Tim Eaton, Jonathan Grenier і David Layman обґрунтували «необхідність дослідження

кореляційної залежності класифікації кібербар'єрів в обліку та специфічних методів їх уникнення чи мінімізації» [8, с. С1]. John Pendley обґрунтував «важливість залучення обліково-контрольних фахівців до розробки програмного і технічного забезпечення у сфері кібербезпеки підприємства» [9, с. 55]. Thomas Heaton Spitters опублікував буклет, «присвячений винятково інструктуванню бухгалтерів у випадках виникнення кіберзагроз, що є першою спробою системно осмислити облікову природу безпекових процесів» [10, с. 4].

Окремі аспекти кібербезпеки облікової інформації досліджувалися науковцями: Nurwanah Andi – виклики для системи обліку [11], Abrahams Temitayo та інші – нормативно-правові та облікові регламенти кіберзахисту [12], Kafi Md Abdullahel, Akter Nazma – взаємозв'язок фінансової та кібербезпеки [13], Dhimas Surya – кібервпливу на облікову професію [14], Boss Scott, Gray Joy, Janvrin Diane – внесення безпекових навчальних курсів у програму підготовки облікових фахівців [15] та інші. Найбільш комплексним і системним дослідженням у сфері облікового позиціонування системи кібербезпеки підприємств є монографія В. В. Муравського «Облік і кібербезпека» [16]. Не дивлячись на значні напрацювання науковців у сфері взаємозв'язку обліку і кібербезпеки, безпекові дослідження окремих облікових об'єктів та процесів не проводяться у належному обсязі. Зокрема, недостатня увага приділяється кіберзахисту облікової інформації про грошові кошти (у тому числі електронні та криптографічні валюти), що є найбільш пріоритетним об'єктом посягання кіберзлочинців. Необхідність організації ефективного кіберзахисту у поєднанні з обліком електронних трансакцій актуалізує тему статті та дає змогу сформувати її мету.

Мета та завдання статті

Мета статті полягає у ідентифікації кіберзагроз функціонуванню системи електронних трансакцій з пропозицією щодо їх усунення через селекцію варіативних організаційних форм забезпечення кібербезпеки підприємства. Для досягнення мети статті необхідна реалізація таких завдань:

- систематизувати напрямки реалізації кіберзахисту облікової інформації про електронні трансакції;
- уточнити способи використання сучасних технологій обробки облікової інформації для кіберзахисту;
- розробити інформаційну схему організації кібербезпеки електронних трансакцій на основі поєднання варіативних форматів організації безпекового підрозділу підприємства.

Виклад основного матеріалу дослідження

Система електронних трансакцій піддається численним кіберризикам, які переслідують різну мету, але націлені на завдання шкоди підприємству. Для подолання кіберзагроз функціонуванню підприємства необхідна систематизація напрямків кіберзахисту електронних трансакцій. Враховуючи явність чи прихованість, внутрішність чи зовнішність, активність чи пасивність кіберзагроз, кіберзахист системи електронних трансакцій можна здійснювати у напрямку забезпечення: конфіденційності, цілісності, доступності, порівнюваності та адресності облікової інформації [17] (табл. 1).

Найбільш розповсюдженою формою кіберзлочинності є заволодіння комерційною таємницею іншого підприємства. Об'єктом кібератаки зазвичай є відомості управлінського обліку про електронні трансакції. Зловмисників може цікавити комплекс облікових відомостей про договірні взаємовідносини та розрахунки з контрагентами. Облікова інформація про електронні трансакції є конфіденційною. Доступ до неї надається обмеженому колу стейкхолдерів, як правило, працівникам та керівникам підприємства.

Незаконне отримання конфіденційних облікових відомостей реалізується через отримання несанкціонованих прав доступу або обходження санкційної системи підприємства. Викрадені дані про електронні трансакція треті особи використовують для одержання економічної вигоди. Під загрозою перебувають клієнтські бази даних, наявність грошових коштів, розрахунки з контрагентами, структура витрат підприємства тощо. Отримані інформаційні масиви можуть бути використаними для впливу на контрагентів підприємства. Учасниками системи

електронних трансакцій, особисті дані яких також можуть бути під загрозою викрадення, є працівники, засновники, власники, пов'язані особи, кінцеві бенефіціари тощо. Для забезпечення ефективного кіберзахисту від викрадення конфіденційної інформації про електронні трансакції доцільно збільшити частку використання електронних грошей та криптовалют. Параметри електронних трансакцій з використанням криптооб'єктів є максимально знеособленими. Особисті відомості про контрагентів майже відсутні у системі електронних трансакцій з використанням криптовалют.

Таблиця 1. Напрямки кіберзахисту облікової інформації про електронні трансакції

№ з/п	Напрям кіберзахисту	Обліково-контрольна інтерпретація	Мета та наслідки кібератаки	Спосіб забезпечення кібербезпеки
	Конфіденційність	Доступ до конфіденційної облікової інформації, що містить комерційну таємницю	Викрадення конфіденційної інформації для використання третіми особами	Біометричне підтвердження особи, використання технології блокчейн
	Цілісність	Корисною для стейкхолдерів є тільки повна та цілісна облікова інформація	Порушення цілісності інформації, що призведе до ухвалення хибних управлінських дій	Запровадження внутрішнього моніторингу, контроль економічної безпеки
	Доступність	Цифровізація обліку і контролю передбачає перманенте використання програмно-технічного забезпечення	Порушення доступності до програмно-технічного забезпечення для завдання іміджевих втрат	Делегування хмарним сервісам, створення додаткових джерел живлення та доступу до Інтернет
	Порівнюваність	Для підтвердження достовірності облікова інформація повинна порівнюватися з еталонними зразками або інформаційними ресурсами про функціонування	Підміна або блокування доступу до порівнювального зразка	Використання технології штучного інтелекту, моніторинг Інтернет-трафіку.
	Адресність	Облікова інформація повинна потрапляти до відповідних фахівців в оптимальному обсязі та у необхідний час	Порушення таблиці адресів доставки, що веде до інформаційного хаосу	Чат-боти зі штучним інтелектом, аутсорсинг

Джерело: виконання автором.

Проте, ще більшою перевагою електронних платежів є перехід до блоково-ланцюгового структурування облікової інформації. При організації обліку і контролю електронних трансакцій доцільно застосовувати технологію блокчейн в обробці інформації про електронні трансакції. Блокчейн забезпечує фрагментацію інформаційних масивів з розподілом елементів між багатьма стейкхолдерами. Викрадення одного інформаційного фрагменту не дає змогу зловмисникам повною мірою інтерпретувати облікову інформацію про електронні трансакції. Блокчейн унеможливлює доступ сторонніх осіб до всієї конфіденційної облікової інформації. І тільки у відповідальних за електронні трансакції працівників виникає

можливість повторної реконструкції цілісної облікової інформації з розрізнених фрагментів. Особи з правом доступу до комерційної таємниці регенерують облікову інформацію про електронні трансакції у класичному форматі.

Інший напрям прояву кіберзагроз, які в більшості випадків є внутрішнього походження, пов'язаний з порушенням цілісності облікової інформації про електронні трансакції. Цілісність даних визнається їх відповідністю між моментами виникнення та споживання стейкхолдерами. У спотворенні інформації про електронні трансакції зацікавлений обліково-управлінський персонал підприємства, який переслідує такі цілі: приховування даних з метою заволодіння грошовими коштами; подання недостовірної інформації для зменшення бази оподаткування; інформаційні маніпуляції для введення стейкхолдерів в обману з метою залучення інвестованих грошових засобів; приховування помилок для уникнення покарання. У певних випадках облікові фахівці можуть цілеспрямовано змінюють первинно отримані облікові дані про електронні трансакції. З метою зменшення імовірності виявлення фактів порушення цілісності облікових даних персонал може вступати в змову з іншими працівниками підприємства. Проте, модифікація змісту чи хронологічності облікових запасів в обліку може відбуватися за вказівкою керівників чи власників підприємства. В такому випадку протиправні дії щодо системи електронних трансакцій вчиняються групою осіб, що може становити загрозу національній кібернетичній та економічній безпеці.

Водночас, у порушенні цілісності системи електронних трансакцій також можуть бути зацікавлені зовнішні зловмисники. Вмішуючись в інформаційну систему підприємства, вони здатні викривлювати чи пошкоджувати облікову інформацію. Робиться це з метою завдання перш за все іміджевої шкоди підприємству. Оприлюднення неправдивих облікових відомостей, наприклад, щодо фінансування сумнівних організацій, неефективного витрачання платіжних засобів, закордонного виведення грошових коштів, може формувати негативну публічну думку. Найбільш кардинальним результатом таких кібердій може бути відмова контрагентів від співпраці, відкликання державних замовлень, бойкот продукції тощо. Все це в кінцевому результаті призводить до значних фінансових збитків та навіть банкрутства підприємства.

Неправдиві облікові відомості про електронні трансакції досить складно піддаються спростуванню, що актуалізує превентивну боротьбу з кіберзагрозами щодо цілісності інформації. Для попередження та уникнення таких кіберризиків доцільно запровадити систему внутрішнього безпекового контролю. Метою контрольної перевірки є перманентний моніторинг облікових даних про грошові операції та зіставлення з відомостями, наведеними у системі електронних трансакцій. Виявлені порушення підлягають оперативному коригуванню, а також покаранню винних осіб.

Найбільш важливим напрямком організації кіберзахисту електронних трансакцій, що залежить від працездатності програмно-технічного забезпечення обліку та контролю, є забезпечення доступності облікової інформації. З метою призупинення фінансово-господарської діяльності підприємства зловмисники можуть блокувати доступ користувачів до обліково-інформаційних ресурсів. Обмеження кіберзлочинцями доступу стейкхолдерів до обліково-контрольної системи реалізується двома основними способами. Найбільш простий варіант завдання шкоди кібербезпеці системи електронних трансакцій є унеможливлення доступу до мережі Інтернет. Несвоєчасне отримання облікових даних про електронні трансакції може призвести до втрати грошових коштів або порушення договірних умов розрахунків з контрагентами. Збільшення часового лагу між моментом виникнення даних про електронні трансакції та реакцією на них облікових й управлінських фахівців є причиною неефективного управління грошовими коштами.

Іншим варіантом кібератак на систему електронних трансакцій є пошкодження або виведення з ладу технічного і програмного забезпечення підприємства. Недієздатність програмних продуктів може призвести до повної втрати облікових відомостей або неможливості виконання персоналом функціональних обов'язків. Від організації оперативного та повного доступу до облікової

інформації залежить цілісність системи електронних трансакцій. Забезпечення доступності до облікової інформації про електронні трансакції потребує реалізації організаційних дій з підготовки резервних програмно-технічних засобів. Заблоковані комунікаційні канали передачі облікових даних миттєво можуть замінюватися дублюючими інформаційними потоками про електронні трансакції. Це реалізується за допомогою використання резервного сервера обробки і передачі облікових даних, а також дублюючих каналів зв'язку з мережею Інтернет.

Іншим способом організації кібербезпеки системи електронних трансакцій є перенесення бази даних та інформаційних функцій до хмарного середовища. Системи електронних трансакцій уже успішно функціонують у хмарному просторі, проте реалізація хмарних обчислень в обліку й контролі потребує від підприємства комплексу організаційних дій. Хмарна обробка та передача облікової інформації забезпечує налагодження ефективного кіберзахисту електронних трансакцій. Забезпечення кібербезпеки делегується операторам хмарних сервісів. Доступ до хмарної бази даних реалізується через численні комунікаційні канали в перманентному режимі, що забезпечує загальну стійкість системи електронних трансакцій на підприємстві.

Не менш важливим напрямком організації кіберзахисту системи електронних трансакцій, якому приділяється недостатньо уваги, є забезпечення порівнюваності облікової інформації. Порівнюваність облікових даних передбачає їх звірку з інформацією інших учасників системи електронних трансакцій. Досить часто оператори грошових операцій чи емітенти електронних грошей (криптовалют) надають технічні відомості для їх перевірки системою обліку електронних трансакцій. Також обліково-управлінський персонал може оприлюднювати звітні показники про рух грошових коштів підприємства з метою забезпечення порівнюваності з обліковими даними за попередні періоди або зі звітністю інших суб'єктів господарювання. Зловмисники можуть замінити дані для проведення порівнювального контролю. Найпростішим способом є підміна звітності підприємства, що офіційно оприлюднюється в публічних джерелах. Неправдиві відомості як база порівняння є загрозою для висновків стейкхолдерів про динамічні процеси на підприємстві. Також ціллю кібератак може стати викривлення порівнювальних даних, що більш позитивно (чи навпаки – негативно) позиціонує підприємство порівняно з конкурентами. Кіберзлочинці можуть блокувати канали порівнювальних відомостей з метою введення в оману стейкхолдерів. Користувачі облікової інформації можуть хибно довіряти відомостям, які фіктивно пройшли порівнювальний контроль. Заміна порівнювальної бази може стати причиною втрати довіри до працівників підприємства або до інших учасників системи електронних трансакцій. Усі кіберзлочини, пов'язані з порівнювальністю даних, націлені на порушення довірчих взаємовідносин між учасниками електронних трансакцій.

Вирішення проблеми порівнювальності облікової інформації про електронні трансакції потребує використання штучного інтелекту. Технологія штучного інтелекту, реалізована в сучасних чат-ботах, здатна автоматично виявляти хибну порівнювальну інформацію. Підміна може бути ідентифікована автоматичними алгоритмами унаслідок невідповідності професійних суджень реальній інформаційній ситуації на підприємстві. Через збереження логічних взаємозв'язків з іншими обліковими даними або нелогічністю порівнювальної бази можна автоматично виявляти факти підміни інформаційних ресурсів. Як наслідок, чат-боти зі штучним інтелектом допомагають у виявлені фіктивних облікових даних, що можуть використовуватися для ухвалення необґрунтованих управлінських рішень.

Водночас, важливим напрямком організації кібербезпеки є забезпечення адресності облікової інформації про електронні трансакції. Під адресністю розуміється передача облікової інформації про грошові операції до стейкхолдера. Адресатом інформації є кінцевий споживач, якому і були призначені інформаційні відомості, що будуть використані з корисною метою.

Дії зловмисників, націлені на порушення принципів адресності облікової інформації про електронні трансакції, пов'язані зі заміною адресата або внесенням хаосу в інформаційний

порядок системи електронних трансакцій. Підміна кінцевого споживача або його дублювання передбачають потрапляння інформаційних ресурсів про електронні трансакції до сторонніх осіб. Наприклад, дані про усі грошові потоки приховано пересилаються конкурентам, зловмисникам чи іншим інституціям усупереч інформаційним регламентам підприємства. В такому випадку конфіденційні дані можуть перманентно потрапляти до небажаних осіб, що потенційно завдає шкоди економічній та кібербезпеці підприємства.

Інформаційний хаос у системі електронних трансакцій є елементом економічного саботажу унаслідок випадкового списання грошових коштів, їх потрапляння до інших отримувачів чи тотального блокування всіх грошових операцій. Підприємство не здатне в такому випадку виконувати свої договірні зобов'язання, що потенційно може призвести до призупинення фінансово-господарської діяльності. Кінцевим наслідком кібератак є порушення ритмічності поставок матеріальних цінностей, втрата грошових коштів, судові позови та відмова від співпраці. Неефективна платіжна політика загрожує банкрутством для підприємства, що і може бути ціллю зловмисників.

Для забезпечення адресності облікової інформації про електронні трансакцій потрібний моніторинг інформаційних потоків. Відслідковування процесів руху інформації від адресанта до адресата дає змогу встановити правомірність інформаційних потоків. На основі попередньо розробленої інформаційної схеми обігу інформаційних ресурсів у перспективі можна ідентифікувати факти відхилень. Виявленні аномалії в інформаційних потоках потребують більш детального аналізу з метою експертної оцінки. В цьому може допомогти технологія штучного інтелекту, яка здатна визначати несанкціоноване потрапляння облікової інформації про електронні трансакції до підозрілих осіб. Сторонні особи зазвичай не є працівниками чи контрагентами підприємства, що передбачає автоматичне блокування такої грошової операції. І тільки після дозволу відповідальної особи з числа працівників підприємства підозріла електронна трансакція буде остаточно виконана. Моніторинг адресності облікової інформації є важливою складовою кіберзахисту системи електронних трансакцій.

Центром моніторингу інформаційних потоків підприємства є контроль поведінки персоналу підприємства, відповідального за електронні трансакції. Поведінковий контроль передбачає перевірку діяльності чи бездіяльності персоналу в інформаційно-комунікаційній сфері. Об'єктом безпекової перевірки є дії персоналу з генерування інформації про електронні трансакції, її використання, передачу та інтерпретацію. Оскільки електронні трансакції засновані на Інтернет комунікаціях, необхідна перевірка усього трафіку в глобальній та локальній мережі інтернет. Для підвищення кіберзахисту індивідуальних телекомунікаційних пристроїв доцільним є більш широке застосування засобів біометрії. Перед кожним фактом проведення електронної трансакції необхідно верифікувати особу, якій дозволено певний перелік управлінських та інформаційних дій. Біометричне підтвердження особи працівника автоматично відкриває для нього перелік дозволених інформаційно-функціональних можливостей. Завдяки технології біометрії унеможливлюється: використання службових пристроїв іншими працівниками чи сторонніми особами, перевищення службових повноважень, несвоєчасна або відсутня реакція на облікову інформацію про електронні трансакції. Додатково технологію біометрії можна використовувати для системи пропуску працівників на територію підприємства. Стороннім особам без права доступу до конфіденційної інформації можна забороняти або обмежувати перебування у певних приміщеннях підприємства.

Для мінімізації прояву наведених кіберзагроз у сфері обліку електронних трансакцій необхідним є створення безпекового відділу а організаційній структурі підприємства. Оскільки об'єктом більшості кібератак є грошові кошти, то ядром такого безпекового підрозділу повинен стати кіберзахист системи електронних трансакцій. Основною метою функціонування відділу кібербезпеки електронних трансакцій є попередження, уникнення, боротьба та усунення наслідків кіберзагроз у сфері грошового обігу.

Інформаційним фундаментом безпекового відділу є система обліку і контролю на підприємстві. Оскільки електронні трансакції поєднують технічну та економічну інформацію у процесі обігу грошових коштів та криптовалют, важливою сферою організації кіберзахисту є оптимізація облікових процесів. Теорія та практика бухгалтерського обліку чітко визначає перелік загальнодоступної та конфіденційної інформації. Система обліку генерує та постачає інформаційні ресурси про грошові операції та потоки для усіх стейкхолдерів. Натомість, контроль забезпечує довіру користувачів до облікової інформації про електронні трансакції. Контрольні методики лежать в основі безпекового моніторингу грошових операцій. Як наслідок, система ефективного кіберзахисту електронних трансакцій недієва без використання облікових та контрольних методик інтерпретації даних. Обліково-контрольних фахівців необхідно залучати до безпекових процесів. Лише в командній роботі економічного та кібербезпекового персоналу можлива реалізація надійної системи економічної й кібернетичної безпеки.

Безпековий підрозділ на підприємстві може бути створений у два способи: функціонального об'єднання фахівців та відокремленої організації. Більш простий в реалізації є перший організаційний варіант, який передбачає залучення різних фахівців до кіберзахисту без створення окремої організаційної одиниці в структурі підприємства. Усі працівники окрім виконання основних функціональних обов'язків додатково залучаються до кіберзахисту системи електронних трансакцій. В умовах, коли кількість електронних трансакцій є незначною, а потенційна втрата конфіденційної інформації не здатна суттєво вплинути на діяльність підприємства, функціональне об'єднання фахівців значно мінімізує витрати на забезпечення кібербезпеки. У перелік посадових обов'язків таких працівників доцільно додати ще й безпекові повноваження. Проте ефективність кіберзахисту електронних трансакцій у такому форматі може бути низькою унаслідок несвоєчасної реакції на кіберзагрози.

Більш ефективною формою кіберзахисту системи електронних трансакцій є створення окремого підрозділу з штатними працівниками служби безпеки підприємства. Постійнодіючий підрозділ краще інтегрується в інформаційну систему підприємства. Розподіл функцій з кіберзахисту забезпечує відповідальність працівників безпекового відділу за результати функціонування системи електронних трансакцій. Кожний безпековий працівників повинен підписати трудовий договір з встановленням відповідальності за кіберзахист підприємства. Проте, виокремлення організаційної одиниці призводить до збільшення витрат на її утримання. Тому створення додаткового безпекового підрозділу є доцільним для великих підприємств зі значною кількістю електронних трансакцій.

Додатково безпекові фахівці можуть переносити виконання функціонально-інформаційних процедур у хмарне середовище. Разом з хмарним делегуванням безпекових повноважень перспективним варіантом організації кіберзахисту системи електронних трансакцій є аутсорсинг. Аутсорсинг безпекових функцій передбачає залучення сторонніх незалежних інституцій до кіберзахисту. Безпековий аудит стає новою ефективною формою гарантування надійності та захищеності системи електронних трансакцій. Зовнішні контролери можуть не тільки здійснювати періодичну перевірку стану кібербезпеки підприємства, але й брати безпосередню участь у кіберзахисті підприємства. Незалежні контролери можуть періодично ставати частиною безпекової команди підприємств чи його спеціалізованого підрозділу з кіберзахисту електронних трансакцій. Такі фахівці можуть працювати дистанційно, допомагаючи штатним працівникам у протистоянні кіберзагрозам. За потреби безпекові аудитори можуть виїжджати до підприємства з метою фізичної присутності на об'єкті кіберзахисту. Іншим організаційним варіантом є періодичне відрядження безпекових працівників незалежної інституції для їх участі в кібербезпековому підрозділі підприємства. Через систему відряджень такі працівники направляються аудиторськими компаніями до підприємства, яке замовили послуги аутсорсингу, для реалізації безпекових повноважень.

Найбільш ефективним організаційним форматом кіберзахисту електронних трансакцій є одночасний безпековий

моніторинг грошових операцій. В такому випадку, кожна електронна трансакція, яка відповідає певним критеріям, підлягає паралельному внутрішньому та зовнішньому безпековому контролю. Інтеграція функцій власних безпекових працівників (підрозділу) та залучених незалежних експертів створює найбільш дієву систему кібербезпеки. Незалежний моніторинг унеможливлює участь працівників підприємства в змові з метою заволодіння грошовими коштами чи завдання шкоди економічній безпеці підприємства. Також аудиторські компанії здійснюють постійне тестування системи безпеки підприємств і можуть надавати рекомендації з її оптимізації. Проте, повне делегування безпекових повноважень стороннім інституціям неодмінно пов'язане з передачею конфіденційної інформації про електронні трансакції. А це може призвести до додаткового зростання кіберзагроз унаслідок недобросовісної діяльності аутсорсера або втрати облікової інформації під час її передачі до місць обробки.

Як наслідок, дуальне виконання безпекових повноважень збалансовує не тільки кіберризики, але й безпековий бюджет підприємства. Одночасна реалізація безпекових функцій у системі електронних трансакцій мінімізує витрати підприємства не стільки від оптимізації фонду оплати праці, як унаслідок зменшення потенційної шкоди підприємства унаслідок кібератак. Концепція дуального кіберзахисту оптимально інтегрується в кластерний організаційний формат бухгалтерського обліку та контролю. Інформація про кожну електронну трансакцію в довільному та анонімному режимі почергово розсилається до облікових, управлінських внутрішніх та зовнішніх безпекових фахівців. В такому випадку незалежні аудитори здійснюють перевірку ефективності внутрішнього контролю за кожною фінансово-господарською подією. Це створює додатковий позитивний синергетичний ефект для системи обліку, контролю, управління та кібербезпеки підприємства (рис. 1).

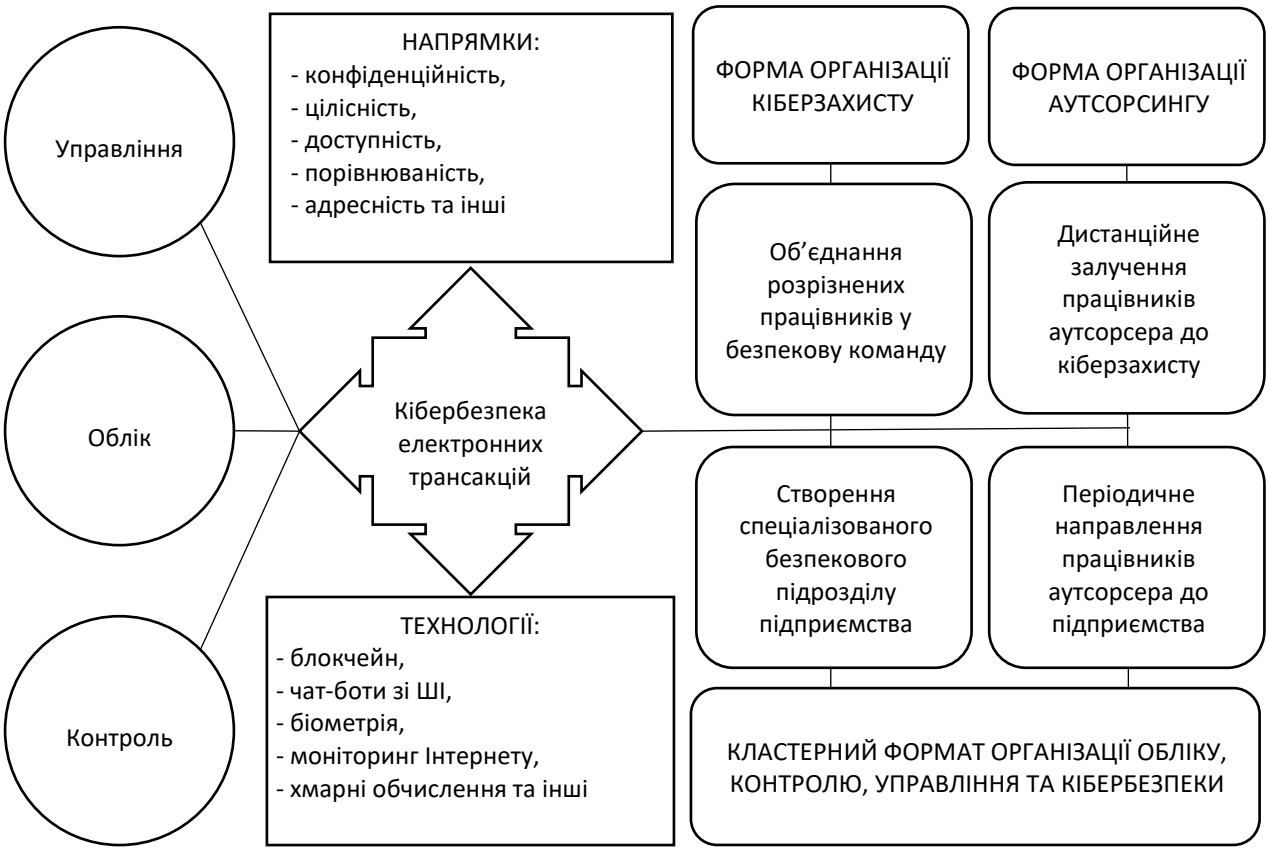

Рис. 1. Організаційні формати кіберзахисту електронних трансакцій

Джерело: розроблено автором

Дуалізація кіберзахисту системи електронних трансакцій фіналізує процес формування суперсистеми підприємства. Інформаційна система електронних трансакцій, заснована на бухгалтерському обліку і контролі, трансформується у ідеальну самокеровану концепцію управління підприємством.

Усі процеси в такій системі настільки оптимізовані, що виключають неефективні управлінські дії працівників, власників та зовнішніх стейкхолдерів. Гармонія досягається в процесах збору, обробки, накопичення, захисту, передачі та інтерпретованого використання облікової інформації про електронні трансакції. Оптимальна система електронних трансакцій стає центром цифровізації варіативних господарських процесів для усіх підприємств, незалежно від розміру бізнесу, галузі діяльності, кількості працівників і т. д. Цифровізація інформаційних процесів у системі електронних трансакцій є шляхом до становлення новітнього постінформаційного суспільства оптимізації в еволюційному розвитку суспільних формацій.

Висновки та перспективи подальших розвідок

Оскільки історично більшість зловмисних дій орієнтувалися на заволодіння грошовими коштами, значної уваги в умовах цифровізації соціально-економічних процесів вимагає кіберзахист електронних трансакцій. В умовах, коли система електронних трансакцій стає основою фінансово-господарської діяльності підприємств, актуалізуються кіберзагрози, які не тільки пов’язані з викраденням грошових коштів (у тому числі електронних чи криптографічних валют). Сучасні кіберзлочини направлені на отримання несанкціонованого доступу до конфіденційної інформації, створення інформаційного хаосу, блокування програмно-технічних ресурсів, суспільну дискредитацію, завдання економічної шкоди підприємству тощо.

Для подолання наведених кіберзагроз функціонуванню системи електронних трансакцій необхідний ефективний її кіберзахист у напрямку забезпечення: конфіденційності, цілісності, доступності, порівнюваності та адресності облікової інформації. При організації кібербезпеки електронних трансакцій доцільно передбачити можливість використання технологій: блокчейн, чат-ботів зі штучним інтелектом, хмарних сервісів обчислення даних, біометричної ідентифікації особи, автоматичного моніторингу інформаційних потоків у бухгалтерському обліку та функціонування служби безпекового контролю. Організація кібербезпеки електронних трансакцій у поєднанні з їх обліком та контролем можлива в організаційному форматі об’єднання розрізнених фахівців у команду або створення спеціалізованого безпекового підрозділу підприємства. Для підприємств, які не мають досвіду у забезпеченні кіберзахисту електронних трансакцій, можливим є безпековий аутсорсинг. Делегування безпекових повноважень може відбуватися у форматі дистанційного залучення працівників незалежного контролера або періодичного їх перебування на території підприємства. Кожний з наведених організаційних форматів має переваги та недоліки, які збалансовуються в умовах інтеграції внутрішнього та зовнішнього безпекового контролю. У рамках кластерної організації обліку і контролю можна перерозподіляти безпекові повноваження між власним відділом кіберзахисту та аутсорсером.

Як наслідок, дуальна організація кіберзахисту електронних трансакцій синергетично мінімізує кіберзагрози та витрати підприємства на кібербезпеку. Такий організаційний варіант кібербезпеки електронних трансакцій адаптивно актуальний для різних видів підприємств. Кіберзахист електронних трансакцій можна трансформувати у систему кібербезпеки підприємства, що потребує подальших безпекових досліджень інших напрямів фінансово-господарської діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мороз Ю. Ю., Цаль-Цалко Ю. С. Облікова політика підприємства та її кібербезпека. 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.
2. Рожелюк В. М. Заходи забезпечення захисту облікової інформації. Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації : зб. наук. праць Національної акад. статистики, обліку та аудиту. 2013. № 2 (12). С. 335–340.
3. Вітер С. А. Світлишин І. І. Захист облікової інформації та кібербезпека підприємства. Економіка і суспільство: електронне фахове видання. 2017. № 11. С. 497–502.
4. Шпак В. А. Організація захисту облікової інформації. Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації. 2015. № 2. С. 181–187.
5. Деньга С. М., Верига Ю. О. Захист інформації в комп`ютерних інформаційних системах бухгалтерського обліку. Бухгалтерський облік і аудит. 2004. № 5. С. 59-65.
6. Грабчук І. Л. Організація захисту облікової інформації в умовах гібридної війни. Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу. 2018. №3 (41). С. 20-24. URL: https://doi.org/10.26642/pbo-2018-3(41)-20-24.
7. Попівняк Ю. М. Кібербезпека та захист бухгалтерських даних в умовах застосування новітніх інформаційних технологій. Бізнес Інформ. 2019. №8. С. 150–157. URL: https://doi.org/10.32983/2222-4459-2019-8-150-157.
8. Eaton Tim, Grenier Jonathan, Layman David. Accounting and Cybersecurity Risk Management. Current Issues in Auditing. 2019. Vol. 13, № 2. C1-C9. URL: https://doi.org/10.2308/ciia-52419.
9. Pendley John. Finance and Accounting Professionals and Cybersecurity Awareness. Journal of Corporate Accounting & Finance. 2018. № 29. P. 53-58. URL: https://doi.org/10.1002/jcaf.22291.
10. Spitters Thomas Heaton. A Supplement to Cybersecurity Breviary for Accountants Kindle Edition. Baume Verlag, San Francisco. 2019. 61 p.
11. Nurwanah Andi. Cybersecurity in Accounting Information Systems: Challenges and Solutions. Advances in Applied Accounting Research. 2024. № 2. P. 157-168. URL: https://doi.org/10.60079/aaar.v2i3.336.
12. Abrahams Temitayo, Ewuga Sarah, Kaggwa Simon, Uwaoma Prisca, Hassan, Azeez. Mastering compliance: a comprehensive review of regulatory frameworks in accounting and cybersecurity. Computer Science & IT Research Journal. 2024. № 5. P. 120-140. URL: https://doi.org/10.51594/csitrj.v5i1.709.
13. Kafi Md Abdullahel, Akter Nazma. Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data Protection. American Journal of Trade and Policy. 2023. № 10. P. 15-26. URL: https://doi.org/10.18034/ajtp.v10i1.659.
14. Dhimas Surya, Doddy Setiawan, Anni Aryani, Taufiq Arifin Cyberattacks on the accounting profession: a literatur review. Media Riset Akuntansi, Auditing & Informasi. 2024. № 24. P. 255-272. URL: https://doi.org/10.25105/v24i2.19953.
15. Boss Scott, Gray Joy, Janvrin Diane. Accountants, Cybersecurity Isn't Just for 'Techies': Incorporating Cybersecurity into the Accounting Curriculum. Issues in Accounting Education. 2022. № 37. URL: https://doi.org/10.2308/ISSUES-2021-001.
16. Muravskyi Volodymyr. Accounting and Cybersecurity: Monograph. Scientific Editor – Z.-M. Zadorozhnyi. Kindle Publishing, KDP, Seattle. USA. 2021. 200 p.

17. Zadorozhnyi Z.-M., Muravskyi V., Shevchuk O. Muravskyi, V. The Accounting System as the Basis for Organising Enterprise Cybersecurity. Financial and Credit Activity: Problems of Theory and Practice. 2020. № 3(34). P. 149-157. URL: https://doi.org/10.18371/fcaptp.v3i34.215462.

REFERENCES

1. Moroz, Yu.Yu., Tsal-Tsalko, Yu.S. (2017). Oblikova polityka pidpryiemstva ta yii kiberbezpeka [Accounting policy of the enterprise and its cyber security]. *Accounting, analysis and control in terms of modern concepts of management of the economic potential and market value of the enterprise*. 4(1), Zhytomyr: Ruta, 8-11 [in Ukrainian].
2. Rozheliuk, V.M. (2013). Zakhody zabezpechennia zakhystu oblikovoi informatsii [Measures to ensure the protection of accounting information]. *Accounting, analysis and auditing: problems of theory, methodology, organization*, 2 (12), 335–340 [in Ukrainian].
3. Viter, S.A. Svitlyshyn, I.I. (2017). Zakhyst oblikovoi informatsii ta kiberbezpeka pidpryiemstva [Protection of accounting information and cyber security of the enterprise]. *Economy and society: electronic specialist publication*, 11, 497–502 [in Ukrainian].
4. Shpak, V.A. (2015). Orhanizatsiia zakhystu oblikovoi informatsii [Organization of protection of accounting information]. *Accounting, analysis and auditing: problems of theory, methodology, organization*, 2, 181–187 [in Ukrainian].
5. Denha, S.M., Veryha, Yu.O. (2004). Zakhyst informatsii v komp`yuternykh informatsiinykh systemakh bukhhalterskoho obliku [Protection of information in computer accounting information systems]. *Accounting and auditing*, 5, 59-65 [in Ukrainian].
6. Hrabchuk, I.L. (2018). Orhanizatsiia zakhystu oblikovoi informatsii v umovakh hibrydnoi viiny [Organization of protection of accounting information in conditions of hybrid warfare]. *Problems of the theory and methodology of accounting, control and analysis,* №3 (41), 20-24. Retrieved from: https://doi.org/10.26642/pbo-2018-3(41)-20-24 [in Ukrainian].
7. Popivniak, Yu. M. (2019). Kiberbezpeka ta zakhyst bukhhalterskykh danykh v umovakh zastosuvannia novitnikh informatsiinykh tekhnolohii [Cyber security and protection of accounting data in the conditions of application of the latest information technologies]. *Business Inform*, 8, 150–157. Retrieved from: https://doi.org/10.32983/2222-4459-2019-8-150-157 [in Ukrainian].
8. Eaton, Tim, Grenier, Jonathan, Layman, David. (2019) Accounting and Cybersecurity Risk Management. *Current Issues in Auditing*, 13 (2), C1-C9. Retrieved from: https://doi.org/10.2308/ciia-52419 [in English].
9. Pendley, John. (2018). Finance and Accounting Professionals and Cybersecurity Awareness. *Journal of Corporate Accounting & Finance*, 29, 53-58. Retrieved from: https://doi.org/10.1002/jcaf.22291 [in English].
10. Spitters, Thomas Heaton (2019). A Supplement to Cybersecurity Breviary for Accountants *Kindle Edition. Baume Verlag, San Francisco* [in English].

11. Nurwanah, Andi. (2024). Cybersecurity in Accounting Information Systems: Challenges and Solutions. *Advances in Applied Accounting Research*, 2, 157-168. Retrieved from: https://doi.org/10.60079/aaar.v2i3.336 [in English].

12. Abrahams, Temitayo, Ewuga, Sarah, Kaggwa, Simon, Uwaoma, Prisca, Hassan, Azeez. (2024). Mastering compliance: a comprehensive review of regulatory frameworks in accounting and cybersecurity. *Computer Science & IT Research Journal*, 5, 120-140. Retrieved from: https://doi.org/10.51594/csitrj.v5i1.709 [in English].

13. Kafi, Abdullahel, Akter, Nazma. (2023). Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data Protection. *American Journal of Trade and Policy*, 10, 15-26. Retrieved from: https://doi.org/10.18034/ajtp.v10i1.659 [in English].

14. Dhimas, Surya, Doddy, Setiawan, Anni, Aryani, Taufiq, Arifin (2024). Cyberattacks on the accounting profession: a literatur review. *Media Riset Akuntansi, Auditing & Informasi*, 24, 255-272. Retrieved from: https://doi.org/10.25105/v24i2.19953 [in English].

15. Boss, Scott, Gray, Joy, Janvrin, Diane. (2022). Accountants, Cybersecurity Isn't Just for 'Techies': *Incorporating Cybersecurity into the Accounting Curriculum. Issues in Accounting Education*, 37. Retrieved from: https://doi.org/10.2308/ISSUES-2021-001 [in English].

16. Muravskyi, Volodymyr. (2021). Accounting and Cybersecurity: Monograph. Scientific Editor – Z.-M. Zadorozhnyi. *Kindle Publishing, KDP, Seattle. USA* [in English].

17. Zadorozhnyi, Z.-M., Muravskyi, V., Shevchuk O., Muravskyi, V. (2020). The Accounting System as the Basis for Organising Enterprise Cybersecurity. *Financial and Credit Activity: Problems of Theory and Practice*, 3(34), 149-157. Retrieved from: https://doi.org/10.18371/fcaptp.v3i34.215462 [in English].

Oleg Shevchuk, PhD in Economics, Associate Professor, Associate Professor, Department of Accounting and Taxation, West Ukrainian National University, Ukraine

Organization of accounting and cyber security of electronic transactions of the enterprise

Abstract

Introduction. Digitization of socio-economic processes has led to an increase in the share of electronic transactions in monetary transactions. Electronic transactions using electronic and cryptographic currencies are the object of increased attention of criminals. The goal of cyberattacks is not only to seize money, but also to steal confidential information, block information flows, create information chaos, damage software and publicly discredit the enterprise. Overcoming various cyber threats requires the organization of an effective system of cyber protection of electronic transactions.

Purpose. The purpose of the article is to identify cyber threats to the functioning of the system of electronic transactions with proposals for their elimination through the selection of variable organizational forms of ensuring the cyber security of the enterprise.

Results. It is proposed to consider accounting and control of electronic transactions as the information basis of the enterprise's cyber security system. The areas of effective cyber protection of electronic transactions are defined, which consist in ensuring: confidentiality, integrity, availability, comparability and addressability of accounting information about monetary transactions. To overcome cyber threats to the functioning of the electronic transaction system, it is proposed to use technologies: blockchain, chatbots with artificial intelligence, biometrics, cloud services, Internet traffic monitoring, etc.

Organizational options for cyber protection of electronic transactions have been systematized in the direction of: uniting disparate employees into security teams or creating a separate security unit of the enterprise; remote involvement of the outsourcer's specialists or their periodic arrival at the enterprise – the customer of outsourcing services. An information scheme of a dual combination of internal and external security control has been developed, which is integrated into the cluster format of the organization of accounting for electronic transactions. It has been proven that

the dualization of cyber security control ensures the balancing of cyber risks and the costs of organizing cyber protection of electronic transactions. This format of cyber security organization is adaptively relevant for various business entities. Taking into account the directions of cyber protection, the capabilities of modern technologies in overcoming cyber risks, the functional powers of security employees, as well as the organizational formats of cyber security of cash flows ensures the reliable functioning of the electronic transaction system at the enterprise. The provision of effective cyber protection in combination with the accounting and control of electronic transactions is fundamental to the organization of a comprehensive cyber security system of the financial and economic activities of the enterprise.

Keywords: accounting; cyber security; cyber risks; security control; electronic transactions; security outsourcing.

Cite as: Shevchuk, O. (2024). Organization of accounting and cyber security of electronic transactions of the enterprise. *Economic analysis,* 34 (3), 403-416. DOI: https://doi.org/10.35774/econa2024.03.403