ВОЛОДИМИР
МУРАВСЬКИЙ

ОБЛІК ТА КІБЕРБЕЗПЕКА

МОНОГРАФІЯ

2023

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ

Володимир Муравський

ОБЛІК ТА КІБЕРБЕЗПЕКА

Монографія

Тернопіль

2023

УДК 657:004
М 91

Рецензенти:

РЕСЛЕР Марина Василівна – д.е.н., професор, декан факультету економіки, управління та інженерії, Мукачівський державний університет;

СТРУК Наталія Семенівна – д.е.н., професор, професор кафедри обліку і аудиту, Львівський національний університет імені Івана Франка;

ФЕСЕНКО Валерія Валеріївна – д.е.н., професор, професор кафедри обліку, аудиту, аналізу і оподаткування, Університет митної справи та фінансів.

За науковою редакцією доктора економічних наук, професора
Зеновія-Михайла Васильовича ЗАДОРОЖНОГО

Рекомендовано до публікації рішенням Вченої ради
Західноукраїнського національного університету
(Протокол № 2 від 25 жовтня 2023 р.)

М 91 **Муравський Володимир.** Облік та кібербезпека : монографія. Тернопіль : ЗУНУ. 2023. 200 с.

ISBN 978-966-654-739-5

У монографії досліджено теоретичні та прикладні аспекти розвитку бухгалтерського обліку у контексті забезпечення кібербезпеки підприємств. Систему бухгалтерського обліку позиціоновано як важливий елемент організації економічної та інформаційної безпеки підприємств. Удосконалено класифікацію кіберризиків у бухгалтерському обліку та користувачів облікової інформації з метою запобігання і усунення кіберзагроз. Розроблено методику обліку окремих облікових об’єктів з використанням комп’ютерно-комунікаційних технологій для кіберзахисту підприємств. Досліджено особливості організації обліку для забезпечення ефективної кібербезпеки підприємств.

Монографія буде корисною для фахівців з бухгалтерського обліку та кібербезпеки, науковців, викладачів, аспірантів, докторантів, студентів економічних і технічних спеціальностей та всіх, хто цікавиться перспективами цифровізації обліку, контролю, управління.

ISBN 978-966-654-739-5

ВСТУП

Формування цифрової економіки, зростання кількості глобальних гібридних конфліктів, повномасштабні військові дії, соціальне дистанціювання та віддалена робота працівників підприємств в умовах пандемії актуалізували системні кіберзагрози на мікро- та макрорівнях. Активний розвиток комп'ютерних і комунікаційних технологій у цифровій економіці призвів до виникнення різноманітних кіберризиків, спрямованих на надання третім особам економічних вигод або завдання економічних збитків через реалізацію цілеспрямованих зловмисних дій або використання вразливостей інформаційної системи підприємства. В інформаційній системі підприємства значної уваги потребує кіберзахист бухгалтерського обліку як основного генератора економічної інформації, яка у більшості випадків є конфіденційною. Забезпечення кібербезпеки передбачає не лише захист облікових даних, але й активне залучення облікових фахівців до безпекових процесів на підприємстві. Бухгалтерський облік, в такому випадку, позиціонується важливим елементом організації ефективного кіберзахисту підприємств.

Організація ефективної кібербезпеки спрямована на попередження, уникнення та усунення наслідків кіберзагроз для системи управління, інформаційною компонентною якої є бухгалтерський облік. Кіберзахист підприємств, секторів і галузей економіки орієнтований на убезпечення облікової інформації та запобігання організаційних, технологічних, іміджевих та інвестиційних втрат через використання специфічних методичних прийомів бухгалтерського обліку. Тому забезпечення кібербезпеки підприємств потребує удосконалення теорії, методології, організації та практики бухгалтерського обліку.

Монографічне дослідження складається з трьох розділів: «Теоретичні передумови взаємозв'язку обліку та кібербезпеки підприємств», «Удосконалення методики обліку для цілей кібербезпеки підприємств», «Організація обліку для забезпечення кіберзахисту підприємств». Монографія призначена для фахівців з мультидисциплінарних досліджень у сфері бухгалтерського обліку та кібербезпеки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ПЕРЕДУМОВИ ВЗАЄМОЗВ'ЯЗКУ ОБЛІКУ ТА КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВ

1.1. Позиціонування системи обліку як елементу організації кібербезпеки підприємств

Важливим елементом запобігання гібридного впливу на національні та державні формації є забезпечення кіберзахисту економічних систем. Кібербезпека підприємств, секторів та галузей економіки передбачає реалізацію інформаційного захисту, попередження організаційних, технологічних, іміджевих та інвестиційних втрат. Враховуючи генеративну природу бухгалтерського обліку у сфері продукування економічної інформації, необхідним є залучення облікових фахівців до проблематики кіберзахисту підприємств. Система бухгалтерського обліку як частина управління підприємством є первинною ланкою в інформаційному процесі, а тому потребує першочергового кіберзахисту.

Спочатку необхідність забезпечення кіберзахисту розглядалася лише як елемент інформаційного кругообігу на підприємствах з метою запобігання: втрати споживчої цінності облікової інформації, потрапляння облікових даних до сторонніх осіб, несанкціонованого доступу працівників до інформаційних ресурсів тощо. Такий, винятково інформаційний підхід до кіберзахисту, є частковим та не дає змоги системно забезпечити кібернетичну безпеку суб’єктів господарювання, галузей економік чи національних економічних систем.

Активатором ґрунтовних науково-прикладних досліджень щодо захисту облікової інформації стали активні кіберзагрози на міждержавному рівні як частина гібридних воєн. Глобальність та масштабність проблематики кібербезпеки визначила необхідність забезпечення інформаційної та економічної безпеки країн. Найвищий рівень кіберзахисту у європейських країн: Великобританії, Естонія, Іспанії [86] (Табл. 1.1).

Таблиця 1.1

Рейтинг країн Європи за рівнем забезпечення кіберзахисту

Країна	Оцінка	Регіональний рейтинг 2021	Глобальний рейтинг 2021	Глобальний рейтинг 2018
Велика Британія	99,54	1	2	1
Естонія	99,48	2	3	5
Іспанія	98,52	3	4	7
Литва	97,93	4	6	4
Франція	97,60	5	9	3
Туреччина	97,50	6	11	20
Люксембург	97,41	7	13	11
Німеччина	97,41	7	13	22
Португалія	97,32	9	14	42
Латвія	97,28	10	15	44
Нідерланди	97,05	11	16	12
Норвегія	96,89	12	17	9
Бельгія	96,25	13	19	30
Італія	96,13	14	20	25
Фінляндія	95,78	15	22	19
Швеція	94,59	16	26	32
Греція	93,98	17	28	77
Австрія	93,89	18	29	28
Польща	93,86	19	30	29
Данія	92,60	20	32	21
Хорватія	92,53	21	33	24
Словаччина	92,36	22	34	45
Угорщина	91,28	23	35	31
Ізраїль	90,93	24	36	39
Північна Македонія	89,92	25	38	34
Сербія	89,80	26	39	58
Кіпр	88,82	27	41	56
Швейцарія	86,97	28	42	37
Ірландія	85,86	29	46	38
Мальта	83,65	30	49	59
Грузія	81,07	31	55	68
Ісландія	79,81	32	58	79
Румунія	76,29	33	62	72
Молдова	75,78	34	63	53
Словенія	74,93	35	67	48
Чехія	74,37	36	68	71
Монако	72,57	37	69	43
Болгарія	67,38	38	77	46
Україна	65,93	39	78	54
Албанія	64,32	40	80	62

Джерело: сформовано автором на основі [85; 86]

З активізацією в останні роки засобів кібернетичного впливу на національні інформаційні середовища, що є частиною гібридних воєн, більшість країн Європи значно покращили своє місце в глобальному рейтингу кібербезпеки. Україна у 2021 році серед країн Європейського контингенту на 39 місці (глобальний показник – 78 місце), що є прийнятним результатом у глобальному вимірі [86].

Досить високе позиціонування України в глобальному рейтингу рівня кібербезпеки пояснюється значною увагою до інформаційного захисту на мікрорівні в умовах активізації воєнних дій. На більшості великих підприємствах національного значення були створені структурні об'єкти або відкриті вакансії для працівників, функціональними обов'язками яких є забезпечення кібернетичної безпеки. Проте, з часом, активні хакерські атаки; викрадення інформації, що містить комерційну таємницю; вбудовування вірусних модулів в програмне забезпечення для отримання вигоди шахрайськими методами і т.д. призвели до актуалізації забезпечення кіберзахисту економічних процесів на усіх підприємствах незалежно від розміру та сфери діяльності.

Проблематиці захисту облікової інформації в умовах прояву активних кіберзагроз на мікро та макро-рівні присвячені праці багатьох науковців. Зокрема, Мороз Ю.Ю. та Цаль-Цалко Ю.С. сформували комплексне розуміння поняття кібербезпека з позиції бухгалтерського обліку, як захищеність життєво важливих інтересів підприємства від внутрішніх і зовнішніх загроз, його кадрового й 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 [23, с. 9]. Вітер С.А. та Світлишин І.І. визначили базові принципи системи заходів кібербезпеки облікової інформації: підтримка програмного забезпечення, охорона конфіденційної інформації, персональна відповідальність, секретність, комплексність, контроль доступу до облікових даних [7, с. 501].

Більшість науковців необхідність кіберзахисту на мікро- та макрорівні пов'язують зі зростанням рівня розвитку комп'ютерно-комунікаційних технологій. У зв'язку з діджиталізацією соціально-економічних процесів та формування кіберпростору виникає підґрунтя для все більшого прояву злочинних дій з метою завдання шкоди або фінансового збагачення. Пріоритетність в обґрунтуванні необхідності активізації кібербезпеки країни відводиться частоті прояву та виду актуальних кіберзагроз. Тобто, основним чинником, який спонукає до зростання рівня кіберзахисту, є імовірність прояву інформаційних бар'єрів та ризиків.

Належно аргументована така позиція у дослідженнях Janvrin Diane, Wang Tawei, які прослідкували хронологію розвитку поняття кібербезпека у частині бухгалтерського обліку. Науковці сформували висновок, що 2019 рік, враховуючи велику кількість кібератак, є переломним у розвитку досліджень щодо захисту системи обліку на підприємстві [100, с.А2]. Підтверджують активізацію наукових досліджень проблематики облікових компонентів кіберзахисту підприємств Haapamäki Elina і Sihvonen Jukka, які відзначають зростання кількості наукових праць з безпекової тематики в 2018-2020 роках пропорційно до зростання кількості кібератак [90, с. 810].

Але, найбільш дискусійною залишається ідентифікація та класифікація заходів подолання інформаційних бар'єрів та загроз функціонуванню систем обліку на підприємстві. Наприклад, Шпак В.А. систематизував чотири групи таких заходів: правові, технічні, програмні та організаційні [41, с. 182–184]. Деньга С.М. та Верига Ю.А. виокремлюють активні і пасивні методики мінімізації загроз інформаційним системам обліку. Активні методи включають попередження комп'ютерних шахрайств та комп'ютерного саботажу, пасивні – уникнення помилок облікових фахівців та поломок програмно-технічного забезпечення бухгалтерського обліку [13, с.62]. Грабчук І.Л. пропонує засоби логічної (розгляд забезпечення інформаційної безпеки підприємства як частини корпоративної культури) та фізичної безпеки

(шифрування даних та фізичний захист технічного забезпечення) [12, с. 23].

Проте, для розуміння економічної природи інформаційної безпеки необхідні більш системні науково-прикладні дослідження, що передбачають встановлення співвідношення між видами кіберзагроз та методами їх подолання. Зокрема, Eaton Tim, Grenier Jonathan, Layman David обґрунтували необхідність кореляційного дослідження класифікації інформаційних бар'єрів та загроз в обліку та специфічних методів управління ризиками на підприємстві [76, с. C1]. Також Попівняк Ю. М. виділила організаційні, кадрові, технічні та юридичні кіберзагрози та відповідні напрямками їх усунення в умовах застосування сучасних інформаційних технологій, таких як блокчейн, хмарна обробка даних тощо [31, с. 156]. Вплив технології блокчейн на організацію кіберзахисту системи бухгалтерського обліку дослідили Demirkan Sebahattin, Demirkan Irem та Mckee Andrew. На прикладі облікової системи в США науковці спрогнозували зростання кількості баз даних великих обсягів («Big data») та обґрунтували важливість структурування та управління ними на основі технології блокчейн для забезпечення інформаційного захисту [70, с.189].

Важливим напрямком дослідження ролі бухгалтерського обліку в забезпеченні безпекових процесів є визначення дій облікових працівників на випадок прояву кіберзагроз. Зокрема, Georg Schaffner Laura, Grove Hugh, Holder Anthony, Clouse Mac розробили інструкції з уникнення, подолання та мінімізації наслідків кібервпливу на економічні системи на підприємстві [81, с.6]. Аналогічно й Рожелюк В.М, розкриваючи заходи мінімізації внутрішніх, випадкових та зовнішніх загроз кібербезпеці, позиціонує кіберзахист підприємства 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 [35, с. 137].

Pendley John пояснив необхідність залучення облікових фахівців до розробки інформаційних технологій (програмного і технічного забезпечення) у сфері кібербезпеки. На думку науковця, ефективне

функціонування системи кіберзахисту економічних процесів неможливе без участі фахівців у сфері обліку та контролю [142, с.55]. Науковці приходять до висновку, що працівники технічних фахових спеціальностей (системні адміністратори, програмісти, корпоративні архітектори, адміністратори баз даних тощо) не здатні забезпечити системний кіберзахист з акцентом на оптимізацію економічних процесів на підприємствах. Spitters Thomas Heaton опублікував окремий буклет, присвячений винятково інструктуванню бухгалтерів у випадках виникнення кіберзагроз. Наукова праця є однією з перших спроб системно осмислити облікову природу безпекових процесів [172, с. 4].

Більшість наукових праць позиціонують систему бухгалтерського обліку як об'єкт забезпечення кібербезпеки підприємств. Такий підхід є науково обмеженим, оскільки не враховує суб'єктність бухгалтерського обліку у забезпеченні кібербезпеки підприємств в умовах розвитку новітніх комп'ютерно-комунікаційних технологій. З метою оптимізації інформаційно-безпекових процесів рекомендовано функції кіберзахисту економічних процесів асоціювати з обліковою системою підприємств.

Забезпечення кібербезпеки передбачає не лише захист облікової інформації, система обліку стає суб'єктом безпекових процесів. Висувається гіпотеза, відповідно до якої бухгалтерський облік є платформою забезпечення кібербезпеки підприємств, інтегратором методичних й організаційних дій з метою реалізації інформаційної та економічної безпеки суб'єктів господарювання, галузей та секторів економіки. Сформована гіпотеза про позиціонування системи бухгалтерського обліку як платформи організації кіберзахисту ґрунтується на емпіричному досвіді підприємств, які практикують заходи із забезпечення інформаційної безпеки.

Базовими причинними постулатами наукової гіпотези визначено, що:

– система бухгалтерського обліку є основним генератором економічної інформації, що визначає пріоритетність забезпечення кібербезпеки облікових процесів;

– значна частина облікової інформації (за виключенням даних, продукованих фінансовим обліком) містять комерційну таємницю,

оскільки використовуються керівництвом підприємства для оперативного, тактичного і стратегічного управління;

– останні хакерські атаки та шахрайські дії реалізовувалися через обліково-управлінське програмне забезпечення (вірус «Pety.A» у програмі «M.E.Doc» [18], відключення енергопостачання населення через хакерські атаки), що пояснює важливість захисту системи обліку;

– сучасні бухгалтери є мультиквалфікованими фахівцями, які поєднують економічні, технічні, юридичні знання і можуть виконувати функції із кіберзахисту підприємств;

– регуляторною базою бухгалтерського обліку є нормативні документи, які визначають більшість інформаційних процесів на підприємстві, і можуть містити регламенти забезпечення кібербезпеки.

Розкриття зазначеної гіпотези щодо розробки методики та організації обліку в частині реалізації кіберзахисту підприємства потребує комплексу науково-прикладних досліджень і розробок (рис. 1.1).

Організація кіберзахисту на платформі системи обліку передбачає розширення функціональних повноважень облікової служби (бухгалтерії) та відділу внутрішнього контролю або введення посади фахівця із кібербезпеки в штат підприємства. Доцільність організаційних трансформацій повинна обґрунтовуватися економічною ефективністю незалежно від розмірів та сфери діяльності суб'єкта господарювання. За даними звіту Internet Security Threat Report на сьогодні 80 % усіх кіберзлочинів адресувалися малим суб'єктам господарювання через використання поштових систем, соціальних мереж та хмарних сервісів [98].

Основним мотиватором кібератак на невеликих за розміром підприємствах є відсутність фахівців чи відділу зі забезпечення кібербезпеки. Відповідно, існує більша імовірність, що кібератаки будуть успішними на малих суб'єктах господарювання. Функції кіберзахисту на таких підприємствах можуть успішно виконувати фахівці відділу обліку чи контролю.

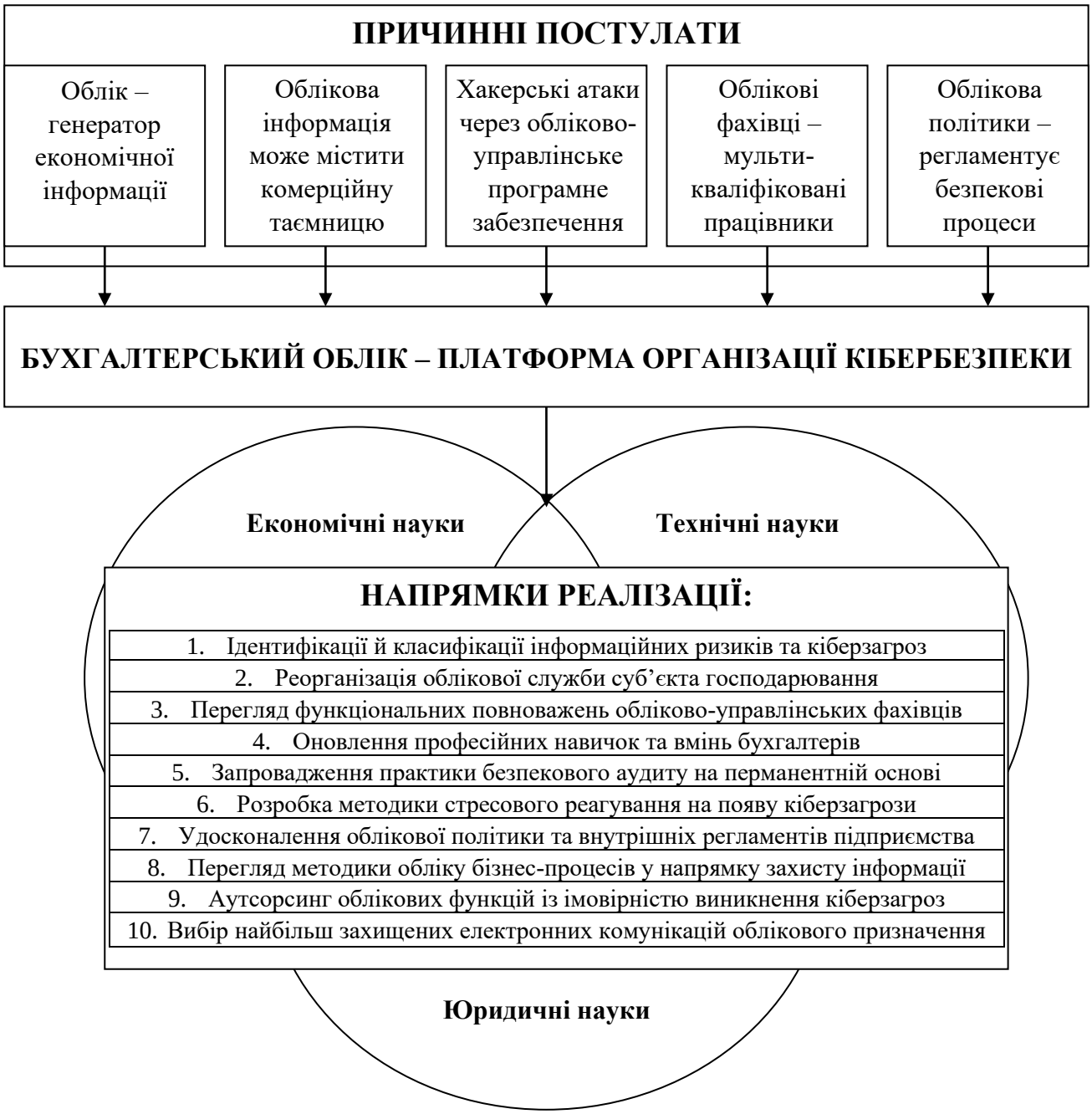


Рис. 1.1. Позиціонування обліку як центру організації кіберзахисту підприємств

Джерело: розроблено автором

Відповідно, посади фахівців із кіберзахисту доцільно поділити на три групи: фахівці з інформаційного захисту (облікові фахівці), працівники служби контролю (фахівці з тестування інформаційних систем на проникнення, аналітики систем забезпечення кіберзахисту, внутрішні контролери, безпекові аудитори, інспектори з організації захисту

конфіденційної інформації), персонал технічного забезпечення (системні адміністратори, адміністратори комп'ютерних мереж, програмісти з спеціалізованих комп'ютерних систем та веб-технологій).

Працівників першої категорії доцільно професійно навчати в рамках освітнього процесу підготовки облікових фахівців. Особами другої групи можуть бути облікові працівники, які мають практичний досвід у сфері кіберзахисту підприємств та здобули додаткові мультидисциплінарні вміння та навички. І лише працівників третьої категорії готують за технічними напрями підготовки фахівців, що не передбачає отримання ґрунтовних знань з економічних дисциплін (у тому числі – обліку, аналізу та контролю).

Таким чином, функціональними обов'язками облікових фахівців першої та другої групи є:

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

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

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

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

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

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

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

– контроль за дотриманням користувачами комп'ютерної інформаційної системи та персоналом підприємства встановлених правил роботи з обліковою інформацією [7, с.501].

Важливою є регламентація функціональних обов'язків із забезпечення кіберзахисту в посадових інструкціях облікових фахівців з визначенням відповідальності за порушення кібербезпеки підприємств. Така відповідальність може бути не лише адміністративною, але й кримінальною у зв'язку ймовірністю завдання шкоди неправомірними вчинками облікових фахівців не лише кібербезпеці окремих підприємств, але й національній безпеці галузі чи сектору економіки.

Додатково визнання відповідальності за реалізацію ефективного кіберзахисту підприємств рекомендовано помістити у Кодекс етики професійних бухгалтерів, який імплементується і в Україні. Зокрема, доцільно розширити зміст принципу надання облікових послуг – конфіденційність (нерозголошення третім особам облікової інформації), в якому ідентифікувати облікового фахівця також як суб'єкта організації захисту облікових даних.

Фіксувати безпекові повноваження в посадових інструкціях облікових фахівців доцільно синхронно із змінами облікової політики підприємства. Регламентація порядку захисту облікової інформації має відбуватися в основному регламенті бухгалтерського обліку – обліковій політиці підприємства. В документі про облікову політику фіксуються різносторонні аспекти функціонування підприємства у частині забезпечення його кібербезпеки.

Якщо суб'єкт господарювання характеризується наявністю значної кількості працівників, складністю структури управління, значними обсягами господарської діяльності, можливий варіант із формування окремих регламентуючих документів за напрямками забезпечення кібербезпеки з реалізацією інформаційної сумісності та єдності з обліковою політикою підприємства. Такі документи щодо регламентації кіберзахисту є основною інструкцією для проведення внутрішнього та зовнішнього безпекового аудиту.

Для перевірки стану інформаційного захисту підприємств доцільно на перманентній основі проводити контроль системи кіберзахисту. За результатами дослідження CyberEdge Group, виявлено, що 78% кіберзагроз на підприємствах, у штаті яких присутні фахівці з

кібербезпеки, були вдалими (близько 63% усіх підприємств піддалися таким загрозам [69, с. 12]. Іншими словами наявність системи кібербезпеки на підприємстві не є гарантією комплексного захисту від усіх загроз. У структурі системи кіберзахисту можуть бути слабкі місця, виявлення яких потребує імплементації безпекового аудиту.

Повноваженнями постійного безпекового аудиту можуть бути наділені внутрішні облікові фахівці або зовнішні незалежні аутсорсери (аудиторські та консалтингові фірми). Основне завдання безпекового аудиту полягає в комплексній системній оцінці інформаційних ризиків, які загрожують економічним процесам, та стану кіберзахисту підприємства. У фахівців служби кіберзахисту повинно бути всебічне розуміння інформаційних процесів на підприємстві, інформаційно-технічної інфраструктури, ситуації щодо взаємодії із зовнішніми стейкхолдерами та контрагентами, алгоритму функціонування спеціалізованого програмного забезпечення для автоматизації управління, юридичних аспектів функціонування суб'єкта господарювання тощо. Усі ці знання в значній мірі акумульовані обліковими працівниками.

Додатково фахівці з бухгалтерського обліку, що не є їм на сьогодні властиве, зобов'язані контролювати: ефективність функціонування брандмауерів, появу новітніх технологій антивірусного програмного забезпечення, стан оновлення спеціалізованих комп'ютерних програм до актуальних версій, а також порядок використання співробітниками надійних паролів для захисту конфіденційної інформації. Комплексне поєднання зазначених вмінь та знань дасть змогу безпековим аудиторам моніторити стан внутрішніх та зовнішніх загроз.

Дієвим методом контролю стану кібербезпеки є тестування інформаційної системи підприємства. Доцільним є проведення ревізії внутрішніх за зовнішніх комунікацій, що дасть змогу проаналізувати потоки інформації на предмет можливого потрапляння до сторонніх осіб. Перманентного контролю потребує продукування та споживання інформації, яка містить комерційну таємницю.

Найбільш трудомістким у безпековому аудиті є тестування персоналу підприємства щодо можливості втрати конфіденційної інформації. Для

безпекових аудиторів доступним є механізм розсилання фішингових повідомлень з метою ідентифікації працівників підприємства, які піддаються впливу кіберзагроз і готові оприлюднювати особисті конфіденційні дані. З виявленими працівниками, що можуть порушити інформаційну безпеку, потрібна подальша робота внутрішніх аудиторів для оновлення безпекових навичок та вмінь. Важливим є також тестування спеціалізованого програмного забезпечення на уразливість до кіберзагроз та антивірусних комп'ютерних програм на здатність виявляти різні види вірусних атак. За результатами тестування програмного забезпечення може прийматися рішення про доцільність його заміни чи оновлення.

Тестування потребує система пропуску та охорони території і приміщень підприємства. Безпекові аудитори можуть контролювати складність доступу до певних територіальних чи внутрішньопросторових одиниць суб'єкта господарювання з метою вироблення рекомендацій щодо покращення служби охорони, пропускної системи, відеоспостереження та біометричної ідентифікації працівників.

У випадку неможливості організації перманентного та ефективного внутрішнього безпекового аудиту керівництво суб'єктів господарювання можуть звертатися до зовнішніх аудиторських фірм. Окрім того, приблизно 84% підприємств за даними Telstra Security Report направляли фахівців з кібербезпеки на перенавчання (оновлення знань), що спричиняло значні адміністративні витрати [176, с.8]. З метою мінімізації витрат на навчання персоналу керівництво підприємств може вдаватися до безпекового аутсорсингу. За даними Інституту дипломованих бухгалтерів в Англії та Уельсі більшість великобританських аудиторських фірм надають послуги з безпекового аудиту [150]. Великі аудиторські компанії активно відкривають вакансії для фахівців з кіберзахисту та сприяють перепідготовці аудиторів з акцентом на забезпечення інформаційного захисту суб'єктів господарювання – замовників аудиторських послуг.

Ринок послуг забезпечення кіберзахисту зростає швидкими темпами. Аудиторські фірми все частіше надають послуги не лише з безпекового

аудиту, але й організації кіберзахисту на підприємствах. Незалежні аутсорсери акумулюють ризики та відповідальність за кібератаки на суб'єктів господарювання. Окрім професійного підходу до забезпечення кіберзахисту безпекові фахівці здатні оперативно реагувати та прояв активних загроз. За даними Telstra у 2019 році 78% підприємств не мають чіткого плану реагування на можливі небезпеки [176, с. 9], а тому потребують участі зовнішніх аудиторів для вироблення безпекової політики на випадок активних загроз.

Саме від своєчасності реакції на кібератаки залежить можливість уникнення інформаційних і, відповідно, економічних та іміджевих втрат. Аудитори здатні самостійно реагувати на деякі кіберзагрози або надавати рекомендації обліковим фахівцям щодо їх усунення. Оперативність антикризового управління в значній мірі залежить від моделі взаємодії між аудиторською фірмою та обліковим відділом підприємства, що потребує ґрунтовних та різноаспектних наукових досліджень безпекового характеру.

1.2. Принципи кібербезпеки облікової інформації

В інформаційному суспільстві та його економічному вимірі – цифровій економіці інформація є основним предметом праці суб'єктів господарювання. Засобом праці все частіше виступає комп'ютерно-комунікаційна техніка, використання якої призводить до прояву кіберризиків. Зловмисників цікавлять інформаційні системи підприємств для завдання економічної шкоди або отримання неправомірної вигоди. Об'єктом кіберінцидентів стає в основному інформація, яка містить комерційний інтерес.

Діяльність зловмисників також орієнтована на викривлення облікової інформації. Через подання часткових чи хибних облікових даних стейкхолдерам можливе завдання економічно шкоди як відправникам, так і одержувачам інформації. На основі некоректної облікової інформації

приймаються неефективні управлінські рішення. Аналогічно й отримання несвоєчасної облікової інформації або блокування доступу до інформаційних ресурсів призводить до запізнілого управління підприємствами.

Враховуючи варіативність кіберризиків, необхідне вироблення єдиних принципів кіберзахисту облікової інформації. Незалежно від виду кібератак важливою є орієнтація на універсальні принципи попередження, уникнення та усунення наслідків загроз безпеці облікової інформації. Принципи є фундаментом вироблення методичних інструкцій в кібербезпеці облікової інформації. Використання стандартизованих правил кіберзахисту підприємств забезпечує ефективне та безризикове управління суб'єктами господарювання.

Принципи обробки та підготовки облікової інформації активно досліджуються науковцями. Більшість з авторів позиціонують якість облікової інформації як визначальну характеристику інформаційних ресурсів. Проте необхідність забезпечення кіберзахисту підприємств актуалізує дещо інший підхід до визначення фундаментального поля обліку. На перше місце у дослідженні принципів підготовки облікової інформації висувається надійність як здатність уникнення та усунення кіберзагроз. Наприклад, Євдокимов В. В. визначає принцип надійності поряд з доступністю та доцільністю як передумови забезпечення економічної безпеки підприємств [15, с. 47]. Надійність як важлива характеристика функціонування інформаційних систем розглядається Saydjari O. у контексті організації ефективної системи кіберзахисту підприємств [157]. Натомість Кирильєва Л.О., Поставний А.О. пропонують принцип конфіденційності облікової інформації, як базис у забезпеченні кіберзахисту підприємств [17], що є дещо обмеженим погляд на проблематику кібербезпеки.

Hentea Mariana визначає основні концептуальні принципи кібербезпеки у складі: ризик, уразливість, загроза, атака, вплив, наслідки та контроль [94]. Проте такий науковий підхід дає змогу виявити концептуальні поняття, які застосовуються у кіберзахисті облікової інформації, а не принципи. Dupuis Marc й Renaud Karen розглядають

етичні принципи кіберзахисту, що пов’язані з подоланням страху перед проявом кіберзагроз [75]. Rosenzweig Paul сформував десять принципів кіберзахисту інформації, які в основному пов’язані з активним розвитком Інтернет-технологій [153]. Проте наведені принципи є застарілі виходячи з сучасного розвитку інноваційних комп’ютерно-комунікаційних технологій та потребують уточнення. Seo Jinsil та інші пояснили вплив сучасних технологій обробки інформації на прикладі віртуальної реальності на трансформацію принципів кіберзахисту підприємств [161]. Аналогічної думки і Badhwar Raj щодо необхідності перегляду консервативних принципів кібербезпеки в умовах імплементації технологій штучного інтелекту [56].

Досить ґрунтоване дослідження провели Легенчук С. Ф., Царук І. М. та Назаренко Т. П., які позиціонують «цілісність», «конфіденційність» та «доступність» як принципи кіберзахисту облікової інформації [19]. Варто зауважити, що наведений список принципів є базовим, але не повним, оскільки не враховує багатоаспектність кіберзагроз підприємств. Зокрема, Kaur Gurdip, Lashkari Ziba та Habibi Lashkari Arash принципи кіберзахисту цілісність, конфіденційність і доступність доповнюють пов’язаними з ними принципами підзвітності та достовірності [103]. Ці ж принципи, тільки в іншій інтерпретації розглядають Kohnke Anne і Shoemaker Dan [106]. Узагальнення наукових напрацювань дає змогу стратифікувати основні принципи кіберзахисту специфічного виду інформаційних ресурсів, якою є облікова інформація.

Наукове позиціонування комерційної таємниці у діяльності суб’єктів господарювання безпосередньо залежить від розвитку ринкової економіки та інституційних трансформацій суспільства. Для країн, які розвиваються, притаманне ототожнення понять комерційної таємниці та конфіденційності інформації. Усі показники фінансово-господарської діяльності засекречуються за умов недобросовісної конкуренції, правової неврегульованості економічних процесів, надмірної державної регламентованості діяльності підприємств тощо. Це спонукає керівництво відносити до складу комерційної таємниці усю інформацію, яка не має ніякого відношення до таємниці як економічної категорії [2, с. 13].

І навпаки, в економічно розвинених країнах, частина конфіденційної інформації, яка має комерційне значення для підприємства, є комерційною таємницею, що потребує налагодження ефективного кіберзахисту. В такому випадку, систему обліку доцільно розглядати з інституційної позиції як ідентифікатора інформації, що є комерційною таємницею. Через поділ обліку та фінансовий та управлінський виокремлюється інформація, що має комерційний інтерес для керівництва підприємства і, потребує обмеженого доступу. Тому на бухгалтерський облік у частині його поділу на фінансовий та управлінський покладається важлива місія визначення переліку комерційної таємниці та забезпечення кіберзахисту конфіденційної облікової інформації.

Законодавче закріплення поділу бухгалтерського обліку на фінансовий (публічна облікова інформація) та управлінський (обмежена облікова інформація) формує первинне правове поле виокремлення інформації, що містить комерційну таємницю. Проте класифікація з позиції кіберзахисту є досить умовною, оскільки інформація фінансового обліку також може бути конфіденційною. Первинні документи та рахунки обліку у більшості випадків є спільними для різних видів обліку. Додатково все активніше ведуться дослідження щодо інтеграції обліку в умовах автоматизованої обробки облікової інформації, що нівелює деякі видові відмінності.

Облікова інформація про господарську, науково-технічну, фінансову, інвестиційну, маркетингову діяльність містить комерційну таємницю. Використання інформації бухгалтерського обліку забезпечує безперебійну господарську діяльність, отримання позитивних фінансових результатів та досягнення конкурентних переваг на ринку. Потрапляння цієї інформації до сторонніх осіб може призвести до економічних збитків. У випадку використання облікової інформації, яка втратила конфіденційність, для тактичного і стратегічного планування діяльності підприємств може призвести до недотримання фінансово-господарських планів.

Дані деталізованого аналітичного обліку також можуть використовуватися зловмисниками для завдання економічної шкоди або реалізації комерційних цілей. При композиції та стискання даних

фінансового обліку у регістрах обліку, пізніше – у фінансовій звітності, втрачаються деталізовані реквізити господарських операцій. Проте первинні дані у проміжних аналітичних таблицях та документах повно ідентифікують факти господарських подій і явищ, а тому потребують обмеженого доступу. Наприклад інформація про постачальників і покупців, дати поставок, популярність певних видів продукції (робіт, послуг), витрати на інноваційно-технічні розробки, стан зношення обладнання і т.д. може бути цікавою для конкурентів.

Додаткові кіберзагрози можуть виникнути при потраплянні облікової інформації до зловмисників за декілька звітних періодів. З використанням методики динамічного аналізу можна виявляти тенденції у фінансово-господарській діяльності підприємства. На основі прогнозу розвитку суб'єктів господарювання будуються стратегії завдання шкоди підприємству, яке втратило конфіденційну інформацію.

У той же час, не вся інформація може визнаватися комерційною таємницею незалежно від волі облікових та управлінських працівників. Перш за все засекреченню не підлягають установча інформація, яка ідентифікує суб'єктів господарювання, їхнє розташування, засновників і власників, сфери господарської діяльності. Усі види фінансової звітності відповідно до переліку, встановленого національним законодавства країн чи міжнародних об'єднань, є публічними. Аналогічно не можуть бути комерційною таємницею дані про базу оподаткування, нараховані податки та збори, а також погашення заборгованості перед фіскальними інституціями. Інші напрямки діяльності суб'єктів господарювання, що пов'язані з екологічними, соціальними, суспільними інтересами не можуть засекречуватися. Перелік облікової інформації, на яку заборонено накладати обмеження в доступі, може знано збільшуватися для публічних, фінансових, інвестиційних підприємств, а також інституцій з державною формою власності.

Для забезпечення захисту конфіденційної інформації підприємство, в особі його керівництва, як основний генератор та власник комерційної таємниці визначає перелік конфіденційної інформації. Крім того, облікові та управлінські фахівці мають право визначити перелік осіб, які можуть

володіти, розпоряджатися, користуватися такою інформацією, визначити правила обробки інформації та права доступу до неї, а також встановлювати інші умови щодо комерційної таємниці [14].

Ефективний захист комерційної таємниці передбачає облік і контроль доступу осіб до конфіденційної інформації. Доцільно фіксувати особу, час, місце та зміст інформації, яка позиціонується як комерційна таємниця. У випадку втрати конфіденційної облікової інформації можливо виявити перелік підозрюваних осіб, що обумовлює принцип санкціонованості.

Санкціонованість у роботі з обліковою інформацією контролюється через систему надання прав на трансформаційні дій. Тобто, з використанням персоналізованих логінів і паролів, цифрових ключів, ідентифікації особи працівника відбувається надання права обробки облікових даних. Санкціонування обробки інформації є запорукою забезпечення цілісності інформаційної моделі функціонування підприємства. Порушення принципу санкціонованості в обробці облікової інформації відбувається унаслідок викрадення, підміни, підбору засобів ідентифікації осіб. Протиправні дії призводять до отримання несанкціонованого доступу до облікових даних сторонніх осіб, що не передбачене інформаційними регламентами підприємства.

Для притягнення осіб до відповідальності за порушення режиму конфіденційності необхідне попереднє укладання угод про нерозголошення інформації. Традиційно з працівником укладається договір про матеріальну відповідальність, в якому зазначають фінансові санкції за порушення безпекового режиму, крадіжок, шкоди майну підприємства чи недотримання функціональних обов’язків. У випадку порушення договірних взаємовідносин щодо втрати комерційної таємниці може наставати додатково дисциплінарна, адміністративна і кримінальна відповідальність працівників.

До заходів дисциплінарної відповідальності відносять: зауваження, попередження, догана, переведення на іншу роботу та ін. [21]. Адміністративна відповідальність передбачає санкції у вигляді штрафу за порушення, використання, розголошення комерційної інформації з метою

спричинення збитків діловій репутації або майну підприємця [28, с. 59]. Кримінальна відповідальність передбачена за незаконне збирання інформації з метою комерційного шпигунства та за розголошення комерційної таємниці, що призводить до можливого позбавлення волі та відшкодування матеріальних і моральних збитків керівництву підприємства [37].

Виявлення факту втрати конфіденційної інформації потребує автоматичного списання вартості комерційної таємниці з рахунків бухгалтерського обліку. Факт прояву кіберзагроз призводить до зменшення вартості нематеріальних активів, а також гудвілу підприємства. Важливим є вироблення дій щодо подолання наслідків кіберзагроз, що потребує перегляду нової тактики і стратегії розвитку підприємства. Втрата конфіденційної інформації передбачає інформування усіх осіб та суб'єктів господарювання, що пов'язані з комерційною таємницею. Удосконалити також потрібно організаційну структуру підприємства, у тому числі обліковий та безпековий підрозділи. Ідентифікація працівників, що призвели до порушення безпекового режиму, потребує їхнього притягнення до відповідальності. Швидкість дій визначає своєчасність припинення впливу кіберризиків та мінімізацію їхній наслідків. Моніторинг безпекового режиму здійснюється на основі контролю доступу до облікової інформації, що визначає принцип доступності у кіберзахисті підприємства.

Доступність облікової інформації – це можливість отримання доступу обліковими фахівцями та стейкхолдерами до інформації у потрібний момент часу. В умовах повної автоматизації обробки облікової інформації необхідний цілодобовий режим забезпечення доступності. Доступність реалізується через надання облікових даних з варіативних джерел на різних носіях. Через комунікаційні канали облікові дані передаються між етапами їхньої трансформації та демонструються зацікавленим особам. Кіберзагрози орієнтовані на блокування доступу до облікової інформації, що порушує принцип доступності.

Досить часто припинення доступу до облікової інформації зумовлене ненавмисними чинниками, які мають випадковий характер. Наприклад,

відключення чи призупинення подачі електроенергії, перебої з Інтернет-зв'язком, технічна чи програмна відмова обладнання, недосконалі бізнес-комунікації, тимчасова втрата працездатності чи звільнення працівників, відповідальних за обробку облікових даних може призвести до порушення режиму доступності. Блокування доступу до облікових даних може бути результатом зумисних дій зловмисниками. Результатом кібератак на веб-ресурси, бази даних, комунікаційні канали чи інші види програмно-технічного забезпечення підприємств є неможливість отримання зацікавленими особами облікової інформації в обумовлений проміжок часу.

Наслідком блокування доступу до облікової інформації є недотримання часового режиму її передачі до наступного етапу обробки чи споживання. Порушується своєчасність інформаційного процесу та зміщуються цикли обробки облікової інформації. Часовий лаг між етапами збору облікових даних та прийняття управлінських рішень може збільшувати до критичних значень, за яких втрачається цінність інформації для стейкхолдерів.

Особливо для управлінського обліку блокування інформаційного доступу має катастрофічні наслідки, що призводить до перетворення корисної облікової інформації на абсолютну нерелевантні масиви даних. Такі дані не несуть корисності для користувачів, оскільки відображають події зі значним часовим відставанням. Іншими словами облікова інформація є не оперативною, що нівелює переваги використання комп'ютерно-комунікаційної техніки.

З доступністю облікової інформації пов'язаний принцип **адресності**. Облікова інформація має доставлятися в місце її споживання відповідно до часових та змістових вимог. Адресність облікової інформації відображає її цільове призначення щодо потрапляння до певного адресата. Тому направляння облікових даних доцільно розглядати в комплексі з класифікацією стейкхолдерів. Інформація фінансового обліку адресується в основному зовнішнім користувачам, управлінського обліку – зовнішнім користувачам.

У випадку надсилання інформації до хибного користувача втрачається її цінність. Користувач може отримати облікову інформацію, якої не потребує. Натомість корисні для нього облікові дані можуть бути помилково адресовані іншому стейкхолдеру. Метою кібератак для порушення адресності облікової інформації є створення комунікаційного хаосу, що в кінцевому випадку призводить до блокування корисних комунікацій.

Забезпечення доступності облікової інформації потребує функціонування облікового підрозділу в безперервному режимі. Безперервність доцільно реалізувати щодо: роботи програмного і технічного забезпечення підприємства, налагодження комунікаційних каналів зв'язку, унеможливлення перебоїв електропостачання, функціонування персоналу підприємства, попередження та оперативне усунення наслідків кібератак тощо.

У випадку неможливості блокування доступу до облікової інформації кібератаки зосереджуються на завдання шкоди її цілісності. **Цілісність** облікової інформації – це можливість надання зацікавленим особам повної інформації у первісному вигляді без несанкціонованих змін. Цілісною є облікові дані, які пройшли усі етапи обробки відповідно до встановленої методики, внутрішніх регламентів та правил прийнятої облікової політики, посадових інструкцій фахівці з обліку та управління. Цілісна облікова інформація найбільш повно та достовірно відповідає соціально-економічній реальності, в якій функціонує підприємство, після усіх процедур обробки.

Цілісність безпосередньо пов'язана з **повнотою** облікової інформації, що засвідчує її відповідність інформаційним запитам стейкхолдерів. Повною є облікова інформація, яка співставна з інформаційними потребами її користувачів. Стейкхолдери можуть бути задоволені отриманими лише повними обліковими масивами, в іншому випадку – облікова інформація неповна. Іншими словами цілісність є свідченням повної достовірності інформації в момент споживання, що означає відсутність втрат чи несанкціонованих змін окремих її елементів.

Причинами порушення цілісності облікової інформації є випадкові чи умисні дії зацікавлених осіб. Випадковими подіями є помилки у роботі облікового та управлінського апарату підприємства, порушення алгоритму чи застарілість програмного і технічного забезпечення, недостатня компетентність осіб у процесі обробки та ознайомлення з інформацією. Умисні дії для порушення режиму цілісності інформації системи підприємства є результатом кібератак зловмисників. Треті особи можуть перехоплювати інформаційні повідомлення з метою їхнього викривлення, що призведе до хибного інформування зацікавлених осіб. Порушення цілісності облікових даних також може бути свідченням приховування правопорушень персоналом підприємства або маніпулювання інформацією для отримання економічних вигод. Зокрема, на основі викривлення даних фінансового обліку можливо залучити інвесторів, отримати кредитування, зменшити виплати дивідендів, оптимізувати нарахування й сплати податків у незаконний спосіб.

Недотримання принципу цілісності у процесі підготовки інформації управлінського обліку може призвести до некоректного управління. У зв’язку з відсутністю повноти облікової інформації в стейкхолдерів може бути недостатньо інформаційних підстав для прийняття управлінських рішень. Ухвалювати управлінські рішення доводиться в умовах повної або часткової невизначеності. Порушення цілісності інформації управлінського обліку є також причиною появи невпевненості у стейкхолдерів щодо достовірності наданої звітності. Для підтвердження достовірності облікової інформації керівництво підприємства або Стейкхолдери можуть вдаватися до залучення аудиторських послуг. Завданням аудиту в таких умовах є надання впевненості в обліковій інформації та проведення безпекового аудиту для моніторингу стану кіберзахисту підприємства.

Для аудиторського контролю кіберзахисту облікової інформації необхідне забезпечування її перевірюваності. Здатність бути перевіреною (принцип **перевірюваності**) визначає можливість перевірки достовірності облікової інформації з різних джерел. Достовірною є інформація, яка відповідає дійсності. Фахівцям з обліку та кібербезпеки необхідно надати

змогу співставлення облікової інформації з варіативних джерел, нормативно-правових документів чи внутрішніх регламентів, фактичними соціально-економічними подіями тощо.

Найбільш повний перелік засобів забезпечення цілісності облікової інформації надали Легенчук С.Ф., Назаренко Т.П. та Царук І.М., серед яких дієвими заходами є:

– формування і використання адекватної системи контролю бухгалтерських даних, що передбачає незалежні засоби стримування та противаги;

– встановлення персональної відповідальності облікових фахівців за забезпечення належного контролю даних;

– розробка механізму виявлення розбіжностей між первинними документами, обліковими записами та звітністю, і мають бути створені необхідні умови для здійснення коригувальних дій при необхідності;

– забезпечення належного кіберзахисту облікової та інших інформаційних систем підприємства, які використовуються для формування облікової інформації;

– удосконалення інтерфейсу облікового програмного забезпечення з метою реалізації функцій контролю, що забезпечує синхронізацію та взаємоузгодження облікових даних у різних підсистемах;

– використання надійних, стабільних та безпечних комунікаційних каналів передачі облікових даних [19].

Взаємозв’язок фундаментальних принципів кіберзахисту облікової інформації відображено на рис. 1.2.

Принципи кіберзахисту облікової інформації доповнюються іншими принципами фундаментальних наукових теорій. На зовнішньому радіусі концептуального поєднання базових принципів кіберзахисту облікової інформації (конфіденційність, доступність, цілісність) перебувають теоретичні принципи бухгалтерського обліку та принципи інформатики. Дотримання усіх зазначених принципів кіберзахисту забезпечує надійність облікової інформації.

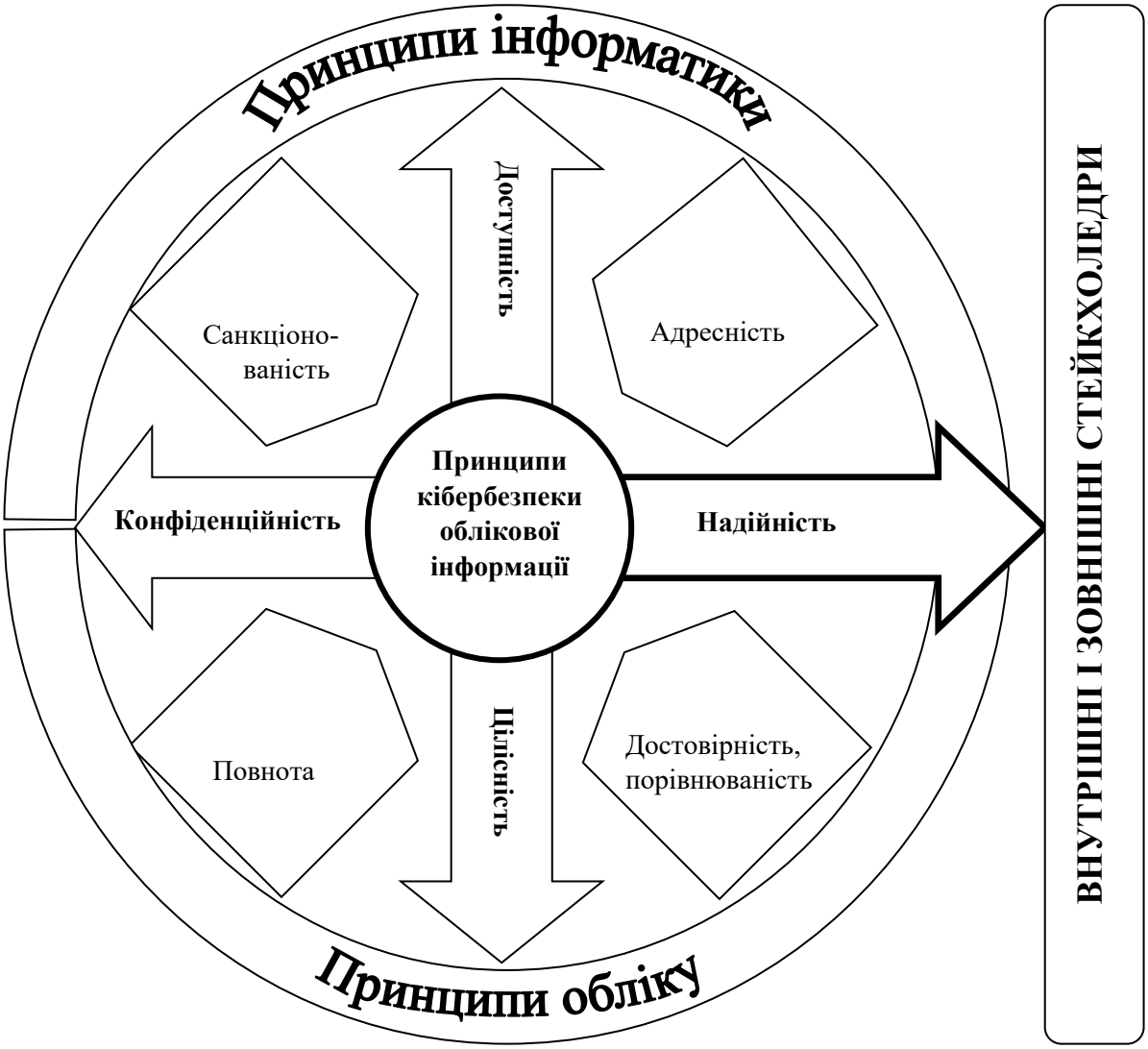


Рис. 1.2. Принципи кібербезпеки облікової інформації

Джерело: розроблено автором

Надійність – це властивість інформації бути безпомилковою, незалежною, неупередженою, адекватною соціально-економічним реаліям. Надійність є суперпринципом в кіберзахисті, який засвідчує відсутність помилок, викривлень, неточностей, спричинених сторонніми особами, а також гарантує доступність та конфіденційність облікової інформації. Лише надійна інформація може бути беззастережно використана стейкхолдерами. Принцип надійності формується на перетині предметних областей інших принципів. Отримання надійної облікової інформації є кінцевою метою комбінованого функціонування облікової та безпекової систем.

1.3. Класифікація кіберризиків в обліку

Оскільки генератором більшості економічних процесів є система обліку на підприємстві, насамперед кіберзахисту потребує облікова інформація. Ускладнення облікових процесів та удосконалення комп'ютерно-комунікаційних процесів є причиною зростання варіативності кіберзагроз. Першочерговим проявом зовнішніх кіберзагроз було викрадення облікової інформації, яка може містити комерційну таємницю. Внутрішні загрози інформаційній безпеці підприємства пов'язані зі зловмисними маніпуляціями обліковою інформацією для одержання економічної вигоди або приховування певних дій чи подій.

Розвиток електронних комунікацій сприяв розповсюдженню комп'ютерних вірусів, зорієнтованих на завдання шкоди системі обліку та управлінню підприємством. Поступово збільшувалася кількість кіберзагроз, пов'язаних з встановленням зловмисного програмного забезпечення для отримання несанкціонованого доступу до облікових даних. Все частіше система обліку стає об'єктом кіберзагроз не лише як комунікаційний канал доступу до критичної інфраструктури підприємства, але й як методика обробки і передачі облікової інформації. Масове використання соціальних мереж та месенджерів призводить до зростання імовірності потрапляння облікових даних до сторонніх осіб. Відповідно активізуються прямі кібератаки на систему обліку підприємства. Додаткового поширення набули шахрайські дії третіх осіб, пов'язані з отриманням неправомірної економічної вигоди.

І лише із удосконаленням методик реалізації гібридних конфліктів кіберзагрози набувають рис комплексності, перманентності, масштабності і, як наслідок, варіативності. Для досягнення успіху в кібератаках використовується комплекс різних кіберзагроз з метою досягнення максимального рівня шкоди суб'єкту господарювання. Такі загрози інформаційній безпеці проявляються на постійній основі, що передбачає імплементацію спеціалізованого підрозділу або штатного фахівця з кіберзахисту в організаційну структуру підприємства. Відповідно виникає необхідність у досліджені поділу кіберризиків за різними

класифікаційними ознаками для реалізації ефективного кіберзахисту облікової інформації.

Науково-публіцистичні джерела інформації з проблематики кіберзахисту підприємств оперують загальноприйнятою класифікацією кіберризиків на: розповсюдження зловмисного програмного забезпечення та вірусів, веб-атаки, атаки веб-додатків, фішинг, відмова обладнання, спам, атаки ботнетів, порушення даних, інсайдерська загроза, фізичні маніпуляції з даними, витік інформації, крадіжки особистих даних, криптоджекінг, розповсюдження програм вимагачів грошей, кібершпигунство та інші [119]. Пандемічні та військові очікування та пов'язана з ними дистанціалізація у виконанні посадових обов'язків призвела до трансформації пріоритетів у реалізації кіберзагроз. Наприклад, дослідження, проведене консалтинговою фірмою Kearney, продемонструвало, що в останні роки зростає кількість кіберзагроз, пов'язаних з делегування інформаційно-функціональних повноважень третім особам [179] (рис. 1.3).

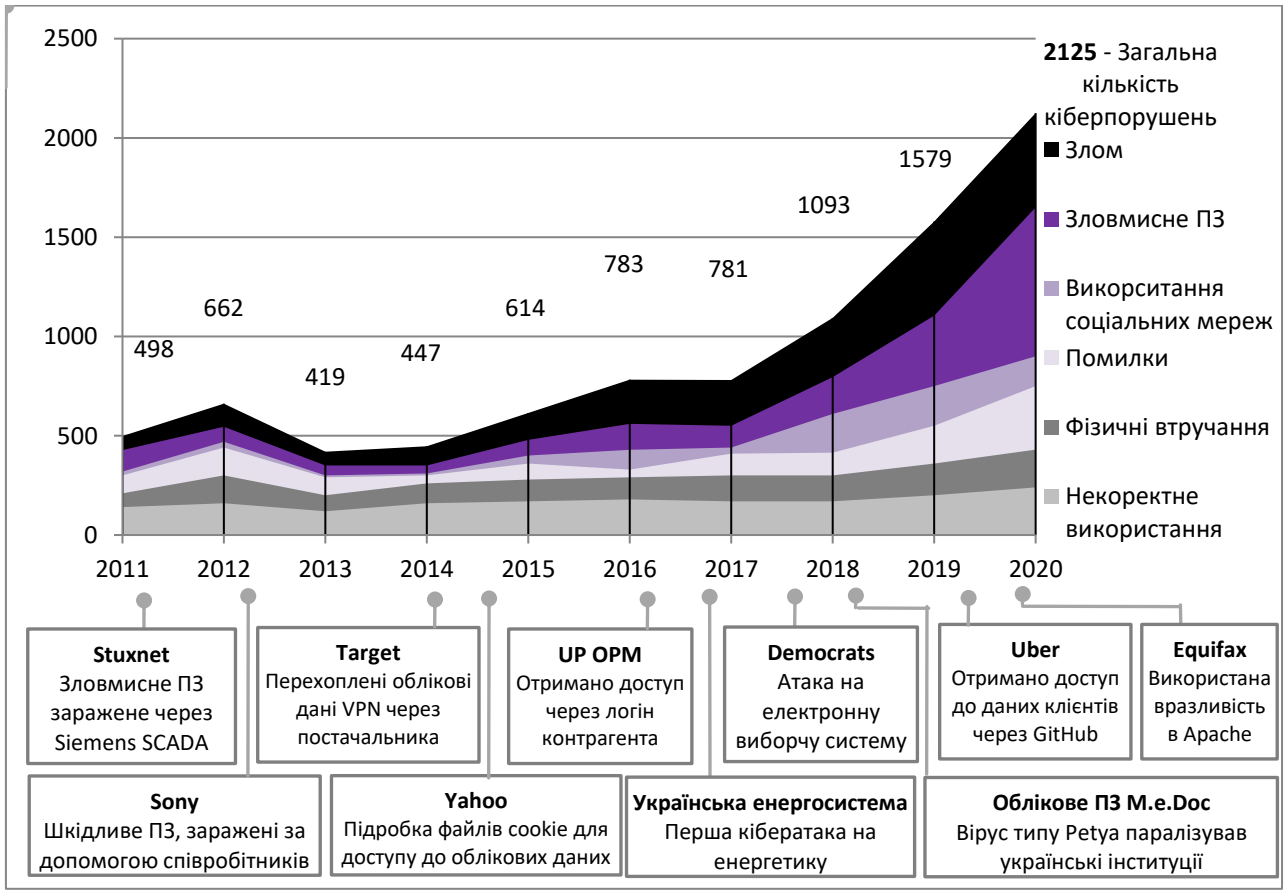


Рис. 1.3. Класифікація великомасштабних кіберзагроз (2011-2020) [179]

Кількість масштабних кібератак, пов'язаних з аутсорсингом за 10 років (2011-2020 р.р.), збільшилася з 498 до 2125 інцидентів. Значна частина кіберзагроз безпосередньо пов'язані з аутсорсингом облікових повноважень. Доцільно виокремити атаки на енергетичний сектор України у 2016 та 2017 році через системи обліку комунальних платежів та розповсюдження вірусу шифратора типу Petya в Україні у 2017 році через оновлення облікового програмного забезпечення.

Цією організацією використовується спрощена класифікація кіберризиків на: злом, зловмисне програмне забезпечення, використання соціальних мереж, помилки, фізичні втручання, некоректне використання.

Натомість, офіційна статистика послуговується класифікацією кіберризиків за формою та методами реалізації. Такий поділ кіберзагроз є малоінформативним для цілей організації кіберзахисту підприємств. Ще у 2012 році Schmitt Michael класифікував кіберконфлікти як частину міжнародних воєнних дій з виокремленням різних кіберзагроз функціонуванню підприємств [158]. Steingartner William та Galinec Darko продовжили дослідження і здійснили розподіл кіберзагроз для виявлення інформаційних ризиків у реалізації гібридного впливу одних країн на інші [173].

Mustafa Nasir обґрунтував активізацію варіативних кіберзагроз в умовах пандемічних очікувань в економіці. Науковець пояснює зміну пріоритетів кібербезпеки підприємств та зростання імовірності прояву різних кіберризиків при продовженні пандемії COVID-19 і військових кризових подій [133]. Asieieva Yu узагальнює кіберризики у контексті вироблення Інтернет-залежності у різних груп користувачів інформації. Акцент зміщений до індивідуальних кіберзагроз, що загрожують економічним та психологічним аспектам функціонування домогосподарств [54, с.28]. Sheehan Barry та інші розробили модель оцінки вразливостей кібербезпеки підприємств на основі класифікації кіберзагроз з визначенням імовірності їхньої активізації для медичних установ Європи [162]. Prakash Febin, Baskar Kala та Sadawarti Harsh позиціонують варіативні кіберзагрози через визначення поняття кіберзлочинність. Класифікація кіберризиків в умовах ідентифікації

кіберзлочинів дала змогу науковцям запропонувати шляхи забезпечення кіберзахисту підприємств [146]. Haque M. та інші систематизували усі кіберризики, що проявляються в умовах використання технології Інтернету речей. Науковці сформували висновок, що при ефективних методиках інформаційного захисту використання технології Інтернету речей можливо уникнути більшості кіберзагроз [91]. Аналогічно й Бараненко Р.В. розкриває класифікаційні особливості кіберзагроз через розмежування понять «кібератака» і «кібертероризм» [58].

Ще менше враховано при класифікації кіберзагроз продукуючу природу бухгалтерського обліку, що є основним генератором економічної інформації на мікро-рівні. В науковому просторі присутні поодинокі праці щодо виокремлення варіативних кіберзагроз у контексті кіберзахисту облікової інформації. Зокрема, Шпаком В.А. розроблено базові складові комплексного забезпечення кібербезпеки підприємства у частині правових, технічних, програмних та організаційних заходів [41, с.185]. Враховуючи, що первинним етапом інформаційного процесу в обліку є збір облікової інформації, активних кіберзагроз зазнає система облікового документування та документообігу підприємства. Документування в бухгалтерському обліку є основою фіксування фінансово-господарських подій та явищ у носіях інформації – документах. Рух документів між відправником та адресатом обумовлюється певною послідовністю, яка іменується документообігом. На усіх етапах документування і документообігу в обліку проявляються специфічні кіберзагрози, які можна об’єднати у групи:

– втрата документу або його складових (додатків, пояснень, окремих листів чи примірників) унаслідок викрадення чи добровільної передачі зловмисникам;

– заміна документів на схожі (аналогічні) примірники з викривленими даними з метою фальсифікації чи завдання економічної шкоди;

– порушення цілісності документа, що обмежує його інформаційне сприйняття;

– помилки при роботі з документами під час їхнього формування та передачі;

– знищення документів для завдання інформаційної та економічної шкоди підприємству [41, с.185].

Але науковцем більшість кіберризиків зводяться до порушення процедур документування й документообігу без врахування багатоаспектності загроз інформаційній та економічній безпеці підприємств.

На противагу дослідженням кіберзагроз, актуальних для облікових документів, Lee GyungMin та інші розвинули ідею поступової активізації безфайлових та, відповідно, бездокументних кіберризиків [113]. Із зростанням цифровізації економіки зменшується потреба у паперових та електронних документах. Сучасні кібератаки все більше загрожують електронним базам облікових даних.

Вітер С.А., Світлишин І.І. систематизували базові принципи (підтримка програмного забезпечення, охорона конфіденційної інформації, персональна відповідальність, секретність, комплектність, контроль доступу) через класифікацію кіберзагроз та заходи (організаційні, технічні й кадрові) зі забезпечення кібербезпеки облікової інформації [7, с. 501]. Але виокремленні постулати кіберзахисту стосуються усіх інформаційних процесів і лише частково враховують облікову специфіку економічних процесів. Аналогічно й Рожелюк В.М. класифікує кіберзагрози на внутрішні та зовнішні з виокремленням різних підвидів, актуальних для бухгалтерського обліку [35]. Але проведене дослідження недостатньо враховує багатоаспектність забезпечення кіберзахисту бухгалтерського обліку. Після узагальнення наукових пропозицій понад двадцяти науковців щодо визначення дефініції «кіберризики» Strupczewski Grzegorz зробив висновок про відсутність напрацювань щодо всебічної класифікації загроз, спрямованих на систему обліку підприємств [175].

Доцільно погодитися з Деньгою С.М. та Веригою Ю.А., що кіберзагрози у бухгалтерському обліку першочергово слід розділяти на дві категорії: навмисні (шахрайство та саботаж) й випадкові (помилки та

катастрофи) [13]. Навмисні кіберзагрози трактуються як цілеспрямована діяльність щодо завдання економічної та інформаційної шкоди суб'єкту господарювання. Навмисні дій завжди є спланованими, підготовленими і зорієнтованими на досягнення чіткої мети. Натомість, випадкові кіберзагрози є наслідком ненавмисних помилок облікових фахівців, нефеефективної системи обліку на підприємстві, недосконалого захисту інформації, невдалої облікової політики підприємства чи програмно-технічних катастроф тощо. Такі загрози не залежать від дій зловмисників і унаслідок випадковості призводять до непрогнозованої втрати (знищення) облікової інформації або створення сприятливих умов для прояву інших кіберзагроз.

Навмисні кіберзагрози поділяються на активні й пасивні. Активними загрозами є завдання шкоди підприємству чи отримання економічної вигоди унаслідок маніпулювання обліковою інформацією. Активні загрози інформаційній безпеці підприємства проявляються у формі кібератак та вірусних інтервенцій, інформаційному шахрайству, інсайдерському саботажу та несанкціонованій передачі облікової інформації. Натомість пасивні кіберзагрози пов'язані з несанкціонованим отриманням облікової інформації. Вони зазвичай латентні, оскільки зорієнтовані на адаптацію та інтеграцію в інформаційне середовища підприємства на тривалий час.

Активні та пасивні кіберзагрози у бухгалтерському обліку не слід безпосередньо асоціювати з внутрішнім та зовнішнім середовищем підприємства. Залежно від просторового прояву кіберзагроз щодо інформаційної системи підприємства доцільно виокремлювати їхні внутрішні, внутрішньосистемні та зовнішні види. Загрози відрізняються походженням та суб'єктністю кіберризиків. Якщо причиною порушення кібербезпеки є працівники чи власники (засновники) підприємства, то кіберризики є внутрішніми. Кіберзагрози, ініційовані особами, які не відносяться до персоналу підприємства, але здійснюють двосторонній інформаційний обмін з системою обліку, є внтурішньосистемними. Такими користувачами облікової інформації є контрагенти, контролюючі інституції, аудиторські та консалтингові фірми, банківські й кредитні

установи тощо. Кіберзагрози, що надходять із зовнішнього середовища від інформаційно та фінансово непов'язаних з підприємством осіб, іменуються зовнішніми.

Аналогічним є принцип класифікації кіберризиків облікової системи за критерієм територіальності. За місцем розташування ініціаторів кіберзагроз за відношенням до суб'єкта господарювання, яке зазначало кібератаки, кіберризики поділяються на: внутрішні (особи перебувають на території суб'єкта господарювання); регіональні (у межах населеного пункту, регіону, області); національні (у країні, об'єднання країн); міжнародні (закордоном).

Проте кіберзагрози обліковій інформації не завжди пов'язані із діяльністю певних внутрішніх чи зовнішніх осіб. Досить часто кіберризики виникають з інших джерел унаслідок бездіяльності або помилок (відмови) програмного й технічного забезпечення. Відповідно за джерелами виникнення загрози обліковій системі можуть бути результатом: діяльності людей, бездіяльності систем й технологій, помилок в інформаційних процесах. Неефективність функціонування програмно-технічного забезпечення на підприємстві може призводити до випадкового витоку конфіденційної інформації, призупинення господарської діяльності та формування «слабких місць» у системі кіберзахисту. Прогалинами у кібербезпеці інформаційної системи підприємства як і помилками в алгоритмі опрацювання облікової інформації можуть скористатися зловмисники для вчинення протиправних дій.

Доповнює наведену класифікацію поділ кіберризиків за походженням. За класифікаційним критерієм генезису кіберзагрози поділяють [8, с. 102] на:

– пов'язані з втратою (пошкодженням, витоком, приховуванням, знищенням) облікової інформації;

– пов'язані з формуванням інформаційного ресурсу (використання недостовірної, неповної, підміненої, викривленої облікової інформації);

– пов’язані з інформаційним впливом (поширення хибної, негативної облікової інформації з метою інформаційного впливу на власників, працівників, контрагентів і т.д. підприємства).

Ідентифікація джерел походження кіберзагроз сприяє розробці сценаріїв їхнього розвитку. На основі сформованої сценарної схеми поширення кіберзагроз відповідно до індивідуальних характеристик функціонування підприємств можливо розробити заходи з превентивного їхнього кіберзахисту.

Проте значно більший вплив на кібербезпеку підприємств здійснює класифікація кіберризиків залежно від об’єктності (загрози інформації чи інформаційній системі підприємства). Ціллю інформаційних кіберзагроз є дані бухгалтерського обліку з метою маніпулятивного отримання до них доступу. Інформаційна інфраструктура залишається поза увагою зловмисників. Натомість загрози інформаційній системі підприємства орієнтовані на отримання вигоди або завдання шкоди суб’єктам господарювання. А облікова інформація використовується лише як засіб отримання доступу до інформаційного середовища підприємства.

Об’єктна множина поділяється на предметні підмножини у класифікації кіберризиків, пов’язаних з: програмним, технічним, кадровим, нормативно-правовим й організаційним забезпеченням. Кожний вид загроз пов'язаний з відсутністю або недостатньою ефективністю певних складових кібербезпеки. Наприклад, загрози програмного забезпечення є результатом помилок при інсталяції та експлуатації комп’ютерних програм для цілей автоматизованої обробки облікової інформації. Загрози технічного забезпечення пов’язані зі застарілістю або неефективним використанням апаратних засобів автоматизації обліку. Кадрові загрози обумовлені недостатньою кваліфікованістю облікового персоналу, а також неможливістю навчання (перенавчання) та відсутністю мотивації до використання сучасних комп’ютерно-комунікаційних технологій. Загрози нормативно-правового забезпечення проявляються унаслідок відсутності можливостей адаптації автоматизованого обліку до вимог внутрішніх та зовнішніх регламентів. Організаційні загрози пов’язані з недоліками у функціонуванні

організаційної структури підприємства – облікового підрозділу, що призводить до випадкових помилок та вразливостей інформаційної системи підприємства.

Відповідно до предметної класифікації кіберзагроз доцільно розробляти заходи щодо їхнього попередження та усунення. Отже, необхідним є використання програмних, технічних, кадрових, нормативно-правових та організаційних заходів кіберзахисту.

З кількістю об’єктів та масштабністю предмету кіберзагроз пов'язаний рівень завданих збитків. За масштабністю кіберзагрози доцільно класифікувати на: загальні, що загрожують функціонуванню суб’єкта господарювання загалом; локальні – напрямкам чи сферам діяльності (основній операційній, адміністративній, збутовій, фінансовій, інвестиційній тощо) підприємства; об’єктні – окремим обліковим об’єктам (необоротним активам, грошовим коштам, доходам тощо) .

Одночасно кіберзагрози необхідно класифікувати за критерієм аспектності. За аспектом кібербезпеки облікової системи кіберзагрози доцільно поділяти на: загрози конфіденційності (облікова інформація стає доступною особам без відповідних повноважень доступу); загрози цілісності (облікова інформація спотворюється, знищується або підмінюється); загрози доступності (обмежується або блокується доступ до облікової інформації).

Через аспектність кіберзагроз реалізуються ризики варіативної форми. За формою реалізації кіберризиків доцільно виокремлювати: кібератаку, кіберінцидент, кібершпигунство, кібертероризм, кібервійну, які відрізняються за мотивацією кібервтручання та методикою його реалізації. Кібератака визначена національним законодавством України як «спрямована (навмисна) дія в кіберпросторі, яка здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або

технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту» [16]. Від кібератаки принципово відрізняються: кіберінцидент (одноразова подія або сукупність випадкових несприятливих подій ненавмисного характеру щодо шкоди обліковій системі підприємства); кібершпигунство (несанкціоноване перманентне багаторазова приховане отримання облікової інформації); кібертероризм (терористична діяльність для зловмисного маніпулювання обліковою інформацією та завдання шкоди підприємству); кібервійна (дестабілізація інформаційної систем підприємства та використання облікової системи для створення хаосу в господарській діяльності підприємств та людей).

Форми кіберзагроз у бухгалтерському обліку відрізняються за латентністю та пролонгованістю інформаційного втручання, що також можуть бути класифікаційними критеріями. Зокрема кібератаки та кіберінциденти є помітними й короткотерміновими; кібершпигунство – прихованими й довготерміновими (або перманентними); кібертероризм та кібервійна – агресивними й довготерміновими.

Відповідно усі кіберризики можливо класифікувати на кримінальні та некримінальні [8, с. 105]. Класифікаційним критерієм є трактування кіберзагроз із позиції кримінальної відповідальності за їхню реалізацію. Ризики облікової системи, що пов’язані з протиправною діяльністю (хакерські атаки, фізичні атаки, шантаж й шахрайство) є кримінальними. Усі решта кіберзагрози у формі антропогенних чи технічних помилок та форс-мажорних обставин іменуються некримінальними.

Врахування кримінальності при досліджені кіберзагроз у бухгалтерському обліку дає змогу виявити наслідки втручання у кібербезпеку підприємств. За кінцевим результатом кіберзагрози доцільно поділяти на такі, що: впливають на інформаційні процеси, викликають труднощі у функціонуванні облікової системи, руйнують систему управління підприємством. Наслідком некримінальних кіберзагроз

переважно є викрадення або викривлення облікової інформації. Натомість кримінальні кіберризики зорієнтовані на блокування окремих інформаційних систем або завдання шкоди функціонуванню суб'єктів господарювання. Відповідно, ризики, що викликають труднощі у функціонуванні облікової системи та блокують систему управління, є руйнівними для підприємства.

Такі кіберзагрози потребують зваженого підходу до організації кіберзахисту у частині уникнення руйнівних ризиків. При превентивному попередженні кіберзагроз важливим є визначення імовірності настання кіберзагроз. За імовірністю кіберзагрози доцільно поділяти на: малоймовірні, ймовірні та неминучі. Відповідно, усі кіберзагрози у бухгалтерському обліку при забезпеченні ефективного кіберзахисту підприємств рекомендовано досліджувати одночасно з оцінкою ймовірності їх прояву. За необхідності, імовірнісна класифікація кіберзагроз може бути доповнена за рахунок поділу на більшу кількість видів ризиків залежно від діапазонів визначення ймовірності настання: відсутня ймовірність (коефіцієнт настання – 0), мала ймовірність (0,1-0,3), середня ймовірність (0,4-0,5), висока ймовірність (0,6-0,8), гарантоване настання (0,9-0,99), неминуче настання (1).

Узагальнена класифікація кіберзагроз у бухгалтерському обліку у розрізі варіативних класифікаційних ознак наведена у табл. 1.2 Залежно від виду кіберзагроз, наведених у таблиці та актуальних для певного суб'єкта господарювання, змінюються заходи із організації кіберзахисту облікової інформації.

Таблиця 1.2

Узагальнена класифікація кіберризиків облікової інформації

№ з/п	Класифікаційний критерій	Вид кіберзагроз
1.	Випадковість	- випадкові, - навмисні.
2.	Цілеспрямованість	- активні, - пасивні.
3.	Інформаційний та фінансовий інтерес	- внутрішні, - внутрішньосистемні, - зовнішні.

продовження таблиці 1.2

4.	Територіальність	- внутрішні, - регіональні, - національні, - міжнародні.
5.	Джерело виникнення	- діяльність людей, - бездіяльність систем й технологій, - помилки в інформаційних процесах.
6.	Походження	пов’язані з: - втратою інформації, - з формуванням інформаційного ресурсу, - з інформаційним впливом.
7.	Об’єктність	- загрози обліковій інформації, - загрози інформаційній системі підприємства.
8.	Предметність	пов’язані з: - програмним забезпеченням, - технічним забезпеченням, - кадровим забезпеченням, - нормативно-правовим забезпеченням, - організаційним забезпеченням.
9.	Масштабність	- загальні, - локальні, - об’єктні.
10.	Аспектність	- загрози конфіденційності, - загрози цілісності, - загрози доступності.
11.	Форма реалізації	- кібератака, - кібершпигунство, - кіберінцидент, - кібертероризм, - кібервійна.
12.	Кримінальність	- кримінальні (хакерські атаки, фізичні атаки, шантаж й шахрайство), - некримінальні (антропогенні помилки, технічні помилки, форс-мажорні обставини).
13.	Пролонгованість	- короткотермінові, - довгострокові, - перманентні.
14.	Латентність	- приховані, - помітні, - агресивні.
15.	Ймовірність	- малоймовірні, - ймовірні, - неминучі.
16.	Наслідки	- впливають на інформаційні процеси, - викликають труднощі у функціонуванні облікової системи, - руйнують систему управління підприємством.

Джерело: систематизовано та удосконалено автором

Використовується також класифікація кіберзагроз у розрізі статі та віку кіберзлочинців. Зокрема, згідно зі статистикою 67 % кіберзагроз є результатом діяльності зловмисників чоловічої статі (вік: до 25 років – 13%, 25-40 років – 39 %, більше 40 років – 15 %) та, відповідно, 33 % - жінки (вік: до 25 років – 6%, 25-40 років – 20 %, більше 40 років – 7 %) [30]. Актуальність вікового та гендерного впливу на класифікацію кіберзагроз наводиться у науковому дослідженні Tsimperidis Ioannis, Yucel Cagatay та Katos Vasilios [181]. Але така класифікація є не надто корисною при виробленні заходів забезпечення кіберзахисту облікової інформації, оскільки пов'язана з ідентифікацією та поділом кіберзлочинців на різні групи, а не кіберризиків.

Наведену класифікацію кіберзагроз доцільно використовувати при організації перманентного кіберзахисту підприємств. Для кожного виду кіберзагроз обліковій інформації притаманна варіативна методика їхнього попередження, уникнення та усунення наслідків. Як наслідок, кіберзахист є динамічним та адаптивним процесом врахування відмінностей у реалізації різних кіберзагроз. Оскільки ускладнення інформаційних процесів та удосконалення комп'ютерно-комунікаційних технологій відбувається перманентно зі зміною соціально-економічних умов функціонування підприємств, запропонована класифікація кіберзагроз облікової інформації потребуватиме доповнення.

1.4. Інноваційна облікова методика забезпечення взаємозв'язку економічної та кібербезпеки підприємств

Більшість кіберризиків у діяльності суб'єктів господарювання пов'язані з викраденням облікової інформації або зменшенням її якісних параметрів. Через дотримання якісних характеристик облікової інформації забезпечується економічна безпека підприємства. Якість інформації є проявом її відповідності очікуванням стейкхолдерів. Порушення будь-якого з якісних параметрів облікової системи може призвести до втрати її

корисності та, відповідно, економічної значимості для внутрішніх та зовнішніх користувачів. Оперування некоректною обліковою інформацією призводить у більшості випадків до економічних втрат підприємства. Прийняття управлінських рішень на основі хибної (викривленої або пошкодженої) облікової інформації є причиною завдання шкоди економічній безпеці підприємства.

Дії внутрішніх користувачів облікової інформації пов’язані з економічною діяльністю підприємства, а зовнішніх – також з функціонуванням інших суб’єктів господарювання. Відповідно, недотримання якісних параметрів системи обліку завдає подвійної економічної шкоди через прямі втрати від діяльності або бездіяльності менеджерів (власників і засновників) та опосередковані збитки чи недоотриману економічну користь від співпраці зі зовнішніми стейкхолдерами. Як наслідок, існує прямий зв'язок між економічною та кібербезпекою підприємств. Реалізація взаємозв’язку економічної та безпекової діяльності передбачає ідентифікацію й дослідження облікових механізмів впливу кіберзагроз на економічну безпеку підприємства.

На рівні підприємства економічна безпека характеризує поточний стан захищеності найважливіших інтересів підприємства від нечесної конкуренції, надмірного тиску з боку контролюючих органів, некомпетентних рішень, недосконалої нормативної бази, а також здатність підприємства до протистояння інформаційним загрозам [11, с.183]. Вплив кіберризиків на економічну безпеку підприємства є предметом наукових пошуків багатьох дослідників. Зокрема, Rodrigues B. та інші доводять, що побічним явищем цифровізації економіки є необхідність забезпечення кібербезпеки. На думку науковців, важливою є розробка дієвих заходів попередження та усунення кіберризиків через прогнозування економічних наслідків недотримання кібербезпеки [151].

Rajput B. розкрив феномен такого поняття як «кіберзлочинність в економічній сфері», що виникло в останні роки через взаємозалежність кіберризиків та економічних наслідків їхньої реалізації. Науковець приходить до висновку, що внаслідок все більшої інтеграції економічного та кіберпростору кількість таких злочинів буде перманентно зростати

[147]. Досліджуючи економічні наслідки різних кіберризиків, Wilson K. та Hugh J. зазначають, що усі сучасні кіберзлочинні дій орієнтовані на отримання певних економічних вигод: глобальне шпигунство, фінансові атаки, шахрайство з картками, крадіжка інформації та фішинг, мережеві атаки та перехоплення трафіку для викрадення інтелектуальної власності, криптографи та вимагачі, крипто-джекінг тощо [184].

Також науковці досліджували способи забезпечення кібербезпеки підприємства у частині мінімізації економічних втрат підприємства. Наприклад, Горбаченко С. обґрунтував доцільність створення єдиної системи національної кібербезпеки, яка об'єднує інформаційне середовище підприємств у єдину інтегровану систему як повноцінну складову національної безпеки на державному рівні [11, с.183-184]. Marasigan R. вказав на важливості інституційних змін в економіці на мікро та макрорівнях для подолання кібернетичних бар'єрів та загроз функціонуванню підприємств [120]. Wilson K. та Hugh J. визначили критично необхідне організаційне, методичне та програмно-технічне забезпечення системи кіберзахисту, яке необхідне для забезпечення стійкої економічної безпеки підприємства [184, с.8].

Rue R., Pfleeger S. запропонували різні моделі економічної оцінки кіберризиків. Науковці пояснили різні механізми впливу кібербезпеки на економічний стан підприємства у частині визначення економічних втрат унаслідок прояву кіберризиків [154, с.54]. Аналогічно й Patterson W. та Gergely M. розробили методику визначення економічної ефективності від організації кібербезпеки підприємства через пояснення впливу кіберризиків на економічні втрати (збитки) або витрати (капітальні й поточні) підприємства [141]. Таким чином, необхідність забезпечення кіберзахисту більшість науковців пов'язують зі зростанням рівня імплементації інформаційно-комунікаційних технологій в інформаційні процеси. Але, зв'язок між активізацією кіберзахисту та зростанням рівня впровадження технологій обробки інформації в соціальні та економічні процеси спростовується проведеним аналізом з використанням глобальних рейтингових даних [85] (рис. 1.4).

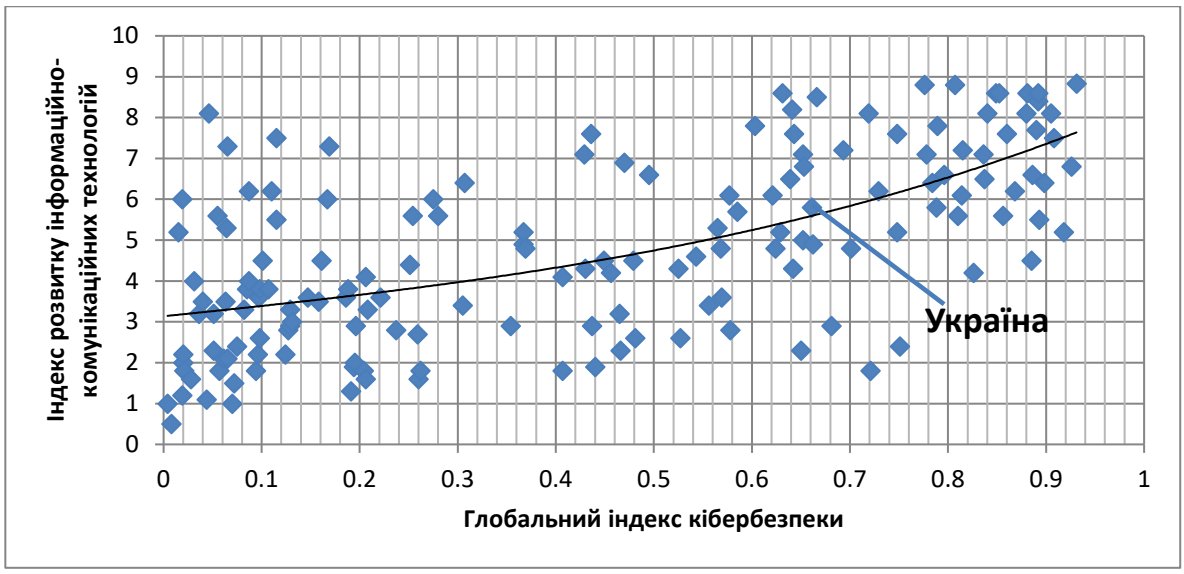


Рис. 1.4. Співвідношення між станом кіберзахисту та рівнем розвитку ІКТ країн

Джерело: розраховано на основі [85]

На основі апроксимованої та згладженої лінії тренду, яка побудована з використанням даних про співвідношення між індексом розвитку комп'ютерно-комунікаційних технологій та індексом кібербезпеки, можливо виявити дисбаланс між цими показниками для багатьох країн. Значне позиційне відхилення наведених у рис. 1.4 значень від усередненої лінії тренду свідчить про відсутність прямої залежності між розвитком ІКТ та станом кіберзахисту у більшості країн.

Більш гомогенний результат отриманий при аналізі співвідношення індексу кібербезпеки почергово з індексом інновацій (рис. 1.5) та індексом мережевої готовності (рис. 1.6) країн. Таким чином, активізація дій щодо забезпечення кібербезпеки обґрунтовується інноваційністю та мережевою готовністю на мікро та макрорівнях. Із зростанням рівня впровадження інновацій та мережевої інфраструктури у національні соціально-економічні процеси виникає необхідність в ефективній системі кіберзахисту.

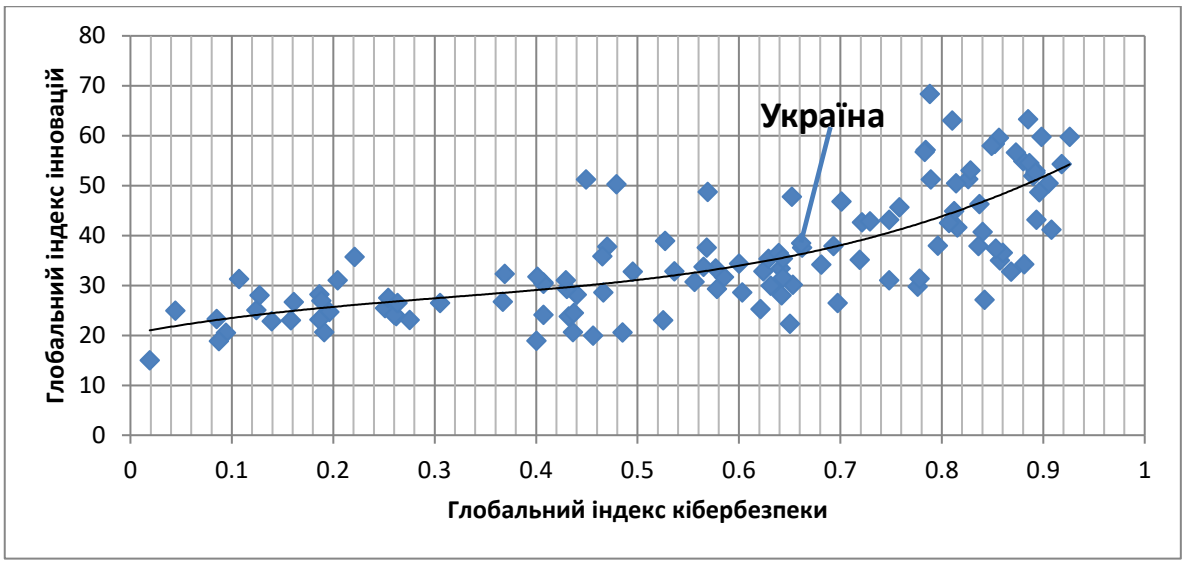


Рис. 1.5. Співвідношення між станом кіберзахисту та рівнем інноваційності країн

Джерело: розраховано на основі [85; 87]

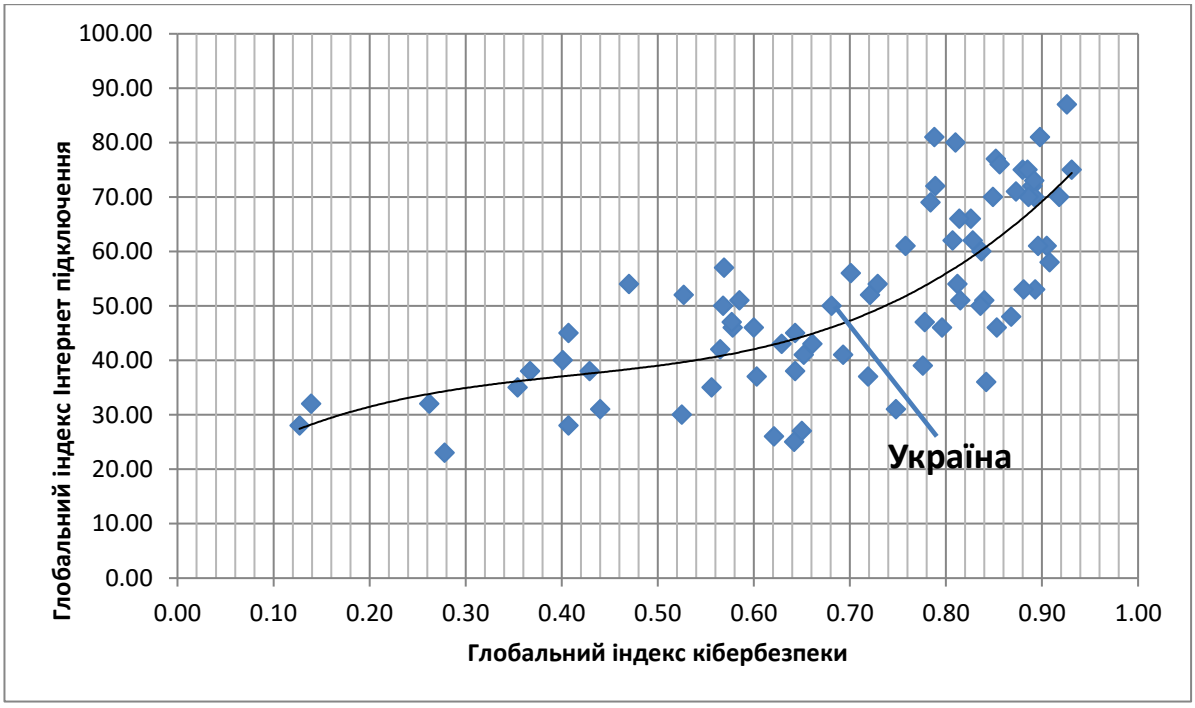


Рис. 1.6. Співвідношення між станом кіберзахисту та мережевою готовністю країн

Джерело: розраховано на основі [84; 85]

Рівень впровадження інновацій та організація мережевої інфраструктури визначає цифрову спроможність країни. На рис. 1.7 відображена пряма залежність між рівнем забезпечення кібербезпеки та

цифровою спроможністю країн, про що свідчать незначні відхилення аналітичних даних від усередненої лінії тренду. Слід зауважити, що деякі країни при незначних показниках інноваційності та цифровізації соціально-економічних процесів займають високі позиції в рейтингу забезпечення кібербезпеки. Наприклад, показники України: Індекс інноваційності – 38,52; Індекс мережевої готовності – 43; Індекс цифрової спроможності – 51,29 при досить високому Індексі кібербезпеки – 0,661, що пояснюється необхідністю протистояння постійним кіберзагрозам унаслідок гібридного іноземного впливу.

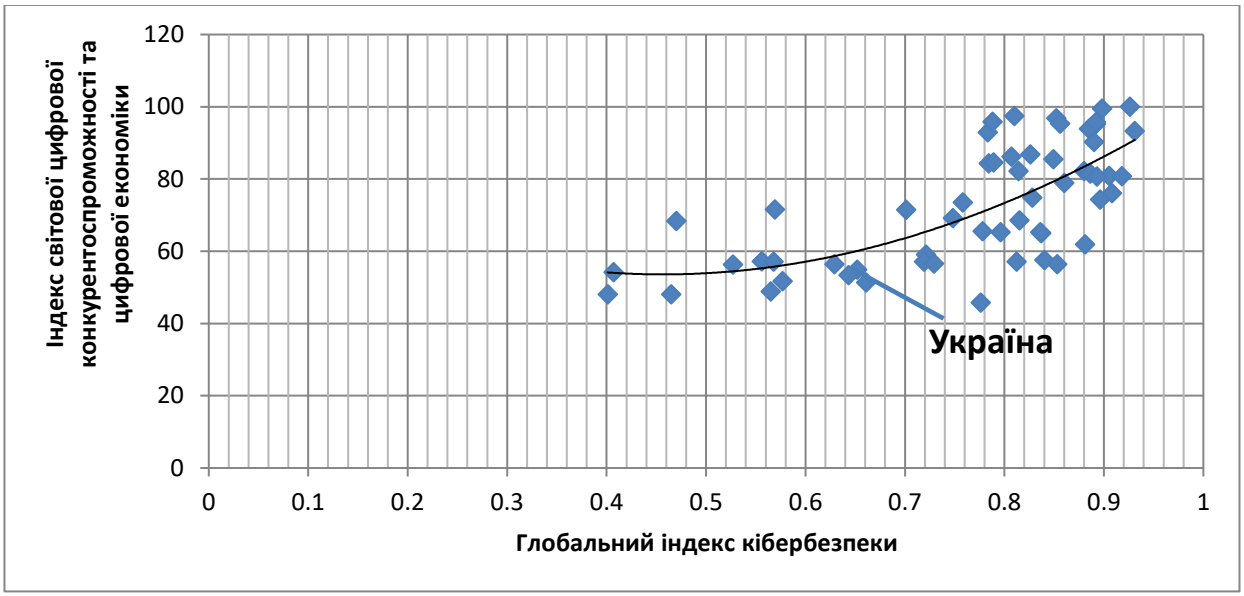


Рис. 1.7. Співвідношення між станом кіберзахисту та цифровою спроможністю країн

Джерело: розраховано на основі [85; 185]

Цифрова спроможність країн є підґрунтям для формування цифрової економіки. Коли більшість соціально-економічних процесів цифровізовані, виникає необхідність у забезпеченні їхньої кібербезпеки. Інформаційним базисом цифрової економіки є управлінський облік. Облікова інформація стає важливим об’єктом кіберзахисту у контексті взаємозв’язку з економічною безпекою країни, галузей та окремих суб’єктів господарювання.

Кібербезпеку в частині облікової політики підприємства, заснованої на забезпеченні економічної безпеки підприємства, Мороз Ю.Ю. та Цаль-

Цалко Ю.С. визначають як захищеність його життєво важливих інтересів та облікової інформації від внутрішніх і зовнішніх загроз, тобто захист підприємства, його кадрового й інтелектуального потенціалу, технологій, прибутку, доданої та ринкової вартості підприємства, який забезпечується системою заходів спеціального правового, економічного, організаційного, інформаційно-технічного і соціального характеру [23, с. 9]. Нехай В. А., Нехай В. В. виокремлюють інформаційну безпеку як важливу складову забезпечення економічної безпеки, що потребує кіберзахисту облікової інформації для дотримання її якісних параметрів [27, с. 138-139].

Євдокимов В.В. позиціонує таку якісну характеристику облікової інформації, як надійність, у контексті забезпечення економічної безпеки підприємства. Надійність, на думку науковця, є характеристикою інформації, яка забезпечує впевненість у доцільності її припущень відносно помилок та тенденції, а також істинності намірів надати всі дані в достовірному вигляді та відповідає принципам: здатності бути перевіреною, достовірності відображення та нейтральності [15, с. 46]. Додатково слід зауважити, що забезпечення надійності облікової інформації в умовах цифрової економіки першочергово передбачає здатність систем обліку уникати та протистояти активності кіберзагроз.

Через розкриття принципів обліку можливо обґрунтувати взаємозв'язок економічної та кібербезпеки підприємств. Активізація та ускладнення кіберризиків потребує перманентної адаптації й трансформації принципів обліку до внутрішніх та зовнішніх умов функціонування підприємства. Оптимізуються способи їхнього практичного втілення (дотримання) задля забезпечення економічної безпеки підприємства. Як наслідок, через принципи обліку відбувається прямий та реверсний вплив кіберризиків на показники фінансово-господарської діяльності суб'єкта господарювання. Особливості реалізації базових облікових принципів в умовах синхронного забезпечення економічної та кібербезпеки, що є першим фундаментальним методологічним рівнем їхнього взаємозв'язку, відображені у табл. 1.3.

Таблиця 1.3

Реалізація принципів обліку та фінансової звітності в умовах забезпечення економічної та кібербезпеки

№ з/п	Принцип обліку та фін. звітності	Реалізація в умовах прояву ризиків економічній та кібербезпеці	Інформаційні наслідки кіберзагроз	Економічні наслідки кіберзагроз
1.	Повне висвітлення	Спотворення, підміна облікової інформації у процесі її передачі внутрішнім та зовнішнім користувачам через неповне (недостовірне) відображення фінансово-господарських явищ та процесів у системі рахунків і звітності.	Фальсифікація облікової інформації при передачі до внутрішніх та зовнішніх користувачів	Отримання економічної вигоди працівниками підприємства або третіми особами
2.	Автономність	Втрата інформаційної самостійності та автономності підприємством через несанкціоноване втручання в інформаційну систему для перманентного моніторингу сторонніми особами інформаційних процесів в обліку та управлінні.	Перманентний несанкціонований доступ до облікової інформації	Промисловий шпіонаж, зменшення економічної самостійності
3.	Послідовність	Порушення послідовності підготовки і подання інформації та реалізації облікової політики, що є причиною несвоєчасного прийняття управлінських рішень	Несвоєчасна обробка облікової інформації	Порушення своєчасності управління
4.	Безперервність	Блокування, призупинення (перервність) фінансово-господарської діяльності підприємства та доведення його до банкрутства.	Блокування інформаційних потоків	Зменшення ринкової вартості, рейдерське захоплення, недобросовісна конкуренція.
5.	Нарахування	Приховування доходів або завищення витрат для уникнення оподаткування, виплати дивідендів тощо.	Фальсифікація облікової інформації для невиконання кредиторських зобов’язань	Фінансові втрати економічно пов’язаних стейкхолдерів-кредиторів.
6.	Превалювання сутності над формою	Викривлення облікових даних у момент їхнього збору та документування через спотворення сутності господарських операцій.	Фальсифікація облікових даних у момент їхнього збору	Отримання економічної вигоди працівниками підприємства або третіми особами
7.	Єдиний грошовий вимірник	Активізація ризиків у сфері електронних транзакцій унаслідок відмови від готівкових коштів на користь криптовалют поза національними валютними системами країн для забезпечення конфіденційності грошових операцій.	Хакерські атаки для доступу до електронних грошових сервісів	Викрадення коштів

Джерело: сформовано автором

Через дотримання фундаментальних принципів обліку відбувається реалізація його функцій щодо забезпечення належної якості облікової інформації. Якістю інформації, продукованої бухгалтерським обліком, є її здатність відповідати вимогам й очікуванням внутрішніх та зовнішніх користувачів. Кіберризики спрямовані на зменшення або блокування придатності облікової інформації до використання через недотримання її якісних параметрів. Забезпечення належної якості облікової інформації визначає якісний рівень взаємовпливу економічної та кібербезпеки підприємств. Основними якісними характеристиками інформації бухгалтерського обліку, на які орієнтовані кіберризики, є: достовірність, своєчасність, доступність, доцільність, надійність, порівнюваність та інші.

Незалежно від інформаційної підпорядкованості якісних параметрів облікової інформації чи їхнього групування за варіативними класифікаційними ознаками, економічна безпека підприємства залежить від активності кіберзагроз. Зокрема, кіберризики зорієнтовані на зменшення якості облікової інформації: достовірності – прийняття некоректних (хибних) управлінських рішень; своєчасності – прийняття запізнілих управлінських рішень; доступності – неможливості отримання чи сприйняття інформації у процесі прийняття управлінських рішень; доцільності – блокування прийняття необхідних управлінських рішень; надійності – неможливість прийняття управлінських рішень у зв’язку з відсутністю довіри до інформації; порівнюваності – прийняття необґрунтованих управлінських рішень через неможливість оцінки та аналізу облікових показників; інших якісних параметрів інформації бухгалтерського обліку – завдання шкоди управлінню підприємством. Отже, реалізація кіберризиків є причиною зменшення ефективності системи управління, що призводить до економічної шкоди підприємству.

Усі якісні параметри облікової інформації в кінцевому випадку пов’язані з дотриманням її конфіденційності в умовах необхідності забезпечення економічної та кібербезпеки підприємства. Інформація бухгалтерського обліку регламентовано розподіляється на загальнодоступну і конфіденційну на основі виокремлення фінансового та управлінського обліку. Ідентифікація об’єктів обліку та поділ його на

види визначає методичний рівень взаємозв'язку економічної та кібербезпеки підприємства.

Конфіденційність даних управлінського обліку обумовлюється виняткова внутрішнім використанням та захистом від потрапляння до сторонніх осіб. Відсутність належного кіберзахисту інформації управлінського обліку може призвести до її використання третіми особами для отримання конкурентної переваги на ринку; залучення покупців і постачальників на більш вигідних комерційних умовах; оптимізації технологічних процесів операційної діяльності; перегляду кадрової, цінової, збутової політики тощо. Порушення режиму конфіденційності, у кінцевому випадку, призводить до економічних втрат підприємства. Економічна шкода унаслідок прояву кіберризиків пов'язана з недоотриманням операційного прибутку унаслідок: втрати ринків збуту, призупинення операційної діяльності; порушення логістичних циклів, недотримання ритмічності виробництва, втрати інтелектуальної власності.

Додатково, використання неправдивої внутрішньої облікової інформації може призвести до прийняття хибних управлінських рішень. Чим вищий рівень управління в ієрархії менеджменту підприємства, тим потенційно масштабніші економічні втрати від прийняття некоректних управлінських рішень. Найбільшої загрози економічній безпеці підприємства може завдати неефективне стратегічне управління унаслідок використання облікової інформації, що зазнала кібератак.

Також активність кіберзагроз залежить від виду облікового об'єкту. Зокрема, найбільше кібератак спрямована на викрадення грошових коштів та їхніх еквівалентів. З аналогічною ймовірністю проявляються кіберзагрози щодо: процесу виробництва і пов'язаних калькуляцій та технологій виготовлення продукції (виконання робіт, надання послуг); основних засобів підприємства для завдання шкоди критичній інфраструктурі та призупинення діяльності підприємства тощо. Натомість такі об'єкти обліку, як виробничі запаси, МШП рідко зазнають кіберзагроз.

Хоча інформація фінансового обліку не містить комерційної таємниці, проте також потребує ефективного кіберзахисту. Оскільки

фінансова звітність офіційно оприлюднюється, виникає загроза її викривлення чи підміни. На основі звітної інформації стейкхолдерами приймаються управлінські рішення щодо реалізації фінансового інтересу до функціонування суб'єкта господарювання. З метою дискредитації підприємства показники його фінансової звітності можуть бути видозмінені унаслідок кібератаки. У момент передачі облікової інформації або у місцях її розміщення можливі зловмисні дії третіх осіб щодо завдання економічної шкоди підприємству.

Оприлюднення неправдивої інформації щодо діяльності суб'єкта господарювання може призвести до втрати економічного інтересу стейкхолдерів. Зокрема, інвестори можуть призупинити подальше інвестування у фінансові інструменти підприємства-емітента; фінансові установи відмовити у кредитуванні; інші кредитори вимагати дострокового погашення кредиторської заборгованості; контрагенти відмовитися від співпраці тощо. Як наслідок, підприємство, показники фінансової звітності якого викривлені, може зазнати непрямої фінансової шкоди, що загрожує економічній безпеці.

З процесом комунікаційної взаємодії зі стейкхолдерами також пов'язаний й комунікаційний рівень взаємовпливу економічної та кібербезпеки підприємства. Кібератаки на комунікаційному рівні зорієнтовані на блокування комунікацій, передачу до користувачів неправдивої або неповної облікової інформації. Стейкхолдери можуть розцінювати такі дії як порушення комунікаційного регламенту або визнавати пошкоджену унаслідок кіберзагроз облікову інформацію за достовірну.

Наприклад, активізація кіберзагроз у комунікаціях підприємства з фіскальними інституціями може призвести до потрапляння неправдивої облікової інформації до адресата. Відмінність облікової інформації щодо бази оподаткування й нарахованих податків (зборів) в обліку підприємства та інформаційній базі податкового органу є причиною фінансових санкцій. Податковий агент зазнає економічних втрат від штрафів за неподання звітності, несвоєчасне чи неповне інформування фіскального органу про фінансово-господарську діяльність. У випадку

відсутності ефективного кіберзахисту комунікацій з контролюючими інституціями зростають загрози економічній безпеці підприємства через перманентні штрафні санкції за порушення фіскальних регламентів.

Прямі кіберризики загрожують банківським комунікаціям. Отримавши доступ до системи обліку електронних трансакцій, зловмисники можуть здійснювати крадіжки коштів з банківських та електронних рахунків. Розмір економічного збитку від прояву таких кіберризиків піддається достовірному визначенню. Несанкціонований доступ до системи обліку безготівкових платежів загрожує економічній безпеці підприємства унаслідок можливості втрати усіх безготівкових коштів. У випадку оперування електронними грошима та криптовалютами пошук зловмисників та повернення втрачених коштів є неможливим. Враховуючи конфіденційність та знеособленість електронних трансакцій, необхідним є превентивне забезпечення ефективного кіберзахисту, оскільки усунення уже активних кіберризиків є ускладненим.

Значних економічних збитків також можуть зазнати суб'єкти господарювання, які користуються послугами облікового та управлінського аутсорсингу. Активні кіберзагрози можуть значно видозмінювати облікову інформацію у процесі комунікаційної передачі від відправника до адресата-аутсорсера. Аутсорсингова фірма на основі отриманих викривлених даних виконує подальші інформаційні процедури обробки, що на кінцевому етапі призводить до формування неправдивої звітності. Зростання кількості етапів обробки облікової інформації, які передані аутсорсеру, унеможливлює відновлення достовірності обліку. А виконання повторних процедур обробки уже достовірної облікової інформації після усунення кіберзагроз потребує додаткових витрат коштів і часу. Також кіберзагрози аутсорсингу збільшують імовірність втрати конфіденційної інформації унаслідок необхідності перманентних електронних комунікацій, що завдає економічної шкоди підприємству. Отже, кількість делегованих облікових функцій одночасно впливає на економічну та кібербезпеку підприємства.

Аналогічних кіберзагроз можуть зазнавати комунікації з аудиторськими фірмами. Неповне інформування аудитора про фінансово-

господарську діяльність підприємства є причиною формування негативного аудиторського висновку або відмови від його надання. Використання такої аудиторської інформації може призвести до формування негативної ділової репутації підприємства в замовника аудиту або інших одержувачів аудиторських документів. Втрата ділової репутації негативно відображається на економічній безпеці підприємства.

Реалізація усіх кіберризиків призводить, у кінцевому випадку, до втрати ділового іміджу підприємства, що визначає репутаційний рівень взаємовпливу економічної та кібербезпеки. Зловмисники можуть завдати репутаційних втрат підприємству опосередковано при досягненні особистих, у більшості випадків фінансових, цілей, або безпосередньо з метою завдання економічної шкоди та призупинення функціонування суб'єкта господарювання. У будь-яких випадках зменшується довіра працівників, контрагентів, інвесторів, кредиторів, суспільних та громадських інституцій до підприємства, яке стало об'єктом кібератак. Репутаційні втрати неодмінно призводять до завдання шкоди економічній безпеці підприємства.

Контролюючі та фіскальні інституції, соціальні й екологічні установи можуть запроваджувати фінансові санкції, блокувати активи підприємства або позиціонувати його діяльність незаконною. Інформаційна взаємодія з такими суб'єктами господарювання визнається «токсичною», що автоматично блокує його фінансово-господарську діяльність. Стейкхолдери облікової інформації у таких випадках втрачають господарський інтерес до суб'єкта господарювання, призупиняють співпрацю, відтерміновують виконання договірних зобов'язань і т.д., що може стати причиною неплатоспроможності, зменшення ліквідності та фінансової стійкості підприємства.

Завдання шкоди діловому іміджу підприємства неодмінно призводить до втрати його ринкової вартості. Знецінюються цінні папери підприємства, зменшується вартість нематеріальних активів. В кінцевому випадку, активізація кіберзагроз призводить до зменшення гудвілу підприємства. Більш детально про вплив якості облікової інформації та використання комп'ютерно-комунікаційних технологій на гудвіл суб'єкта

господарювання розкрито у науковій праці [197]. Найбільш масштабні та системні кібератаки можуть призвести до виникнення унікального явища – негативного гудвілу, коли ринкова вартість компанії менша за сумарну справедливу вартість його активів. Фіналізує завдання кіберризиками шкоди економічній безпеці підприємства його банкрутство або санація. Як наслідок, репутаційний рівень охоплює усі попередні інформаційні ступені взаємовпливу економічної та кібербезпеки (рис. 1.8).

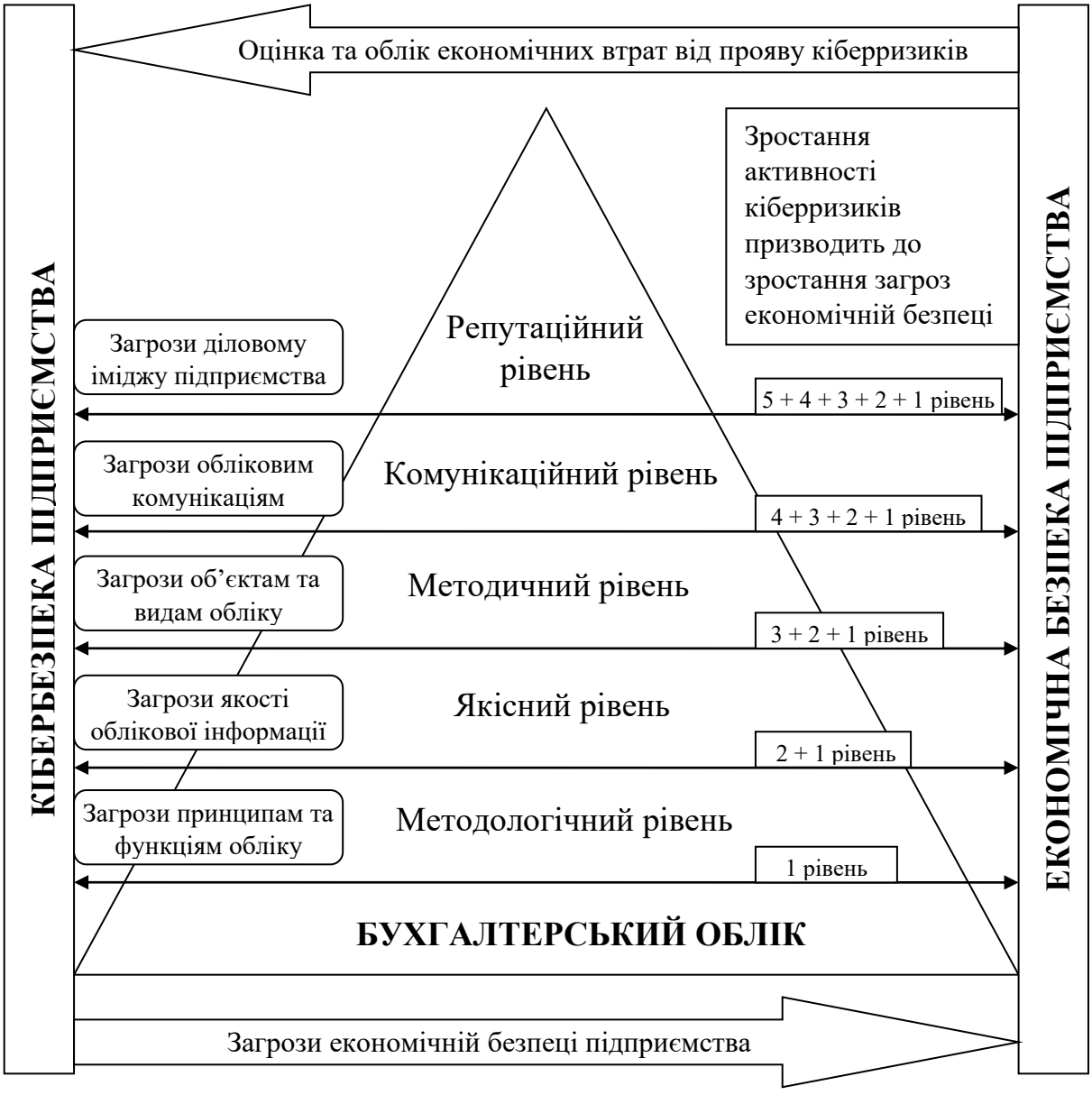


Рис. 1.8. Інноваційна багаторівнева облікова методика взаємовпливу економічної та кібербезпеки підприємств

Джерело: розроблено автором

Кожний наступний рівень взаємовпливу економічної та кібербезпеки підприємств адитивним способом охоплює попередні рівні. Через реалізацію методики бухгалтерського обліку також проявляється зворотній інформаційний зв'язок економічної безпеки з кібербезпекою підприємства. За допомогою облікових методик пізнання економічних процесів можливо достовірно ідентифікувати та оцінити втрати від прояву кіберризиків. Економічні збитки від активізації кіберризиків можуть значно відрізнятися залежно від рівня інформаційного взаємовпливу економічної та кібербезпеки. Значних витрат, пов’язаних з проявом кіберризиків, підприємство зазнає на найвищому репутаційному рівні, що складно піддаються обліковій ідентифікації й оцінці, відповідно потребують подальших наукових досліджень.

1.5. Класифікація стейкхолдерів (користувачів) облікової інформації для цілей кіберзахисту підприємства

Бухгалтерський облік формує інтегроване інформаційне середовище, що поєднує користувачів облікової інформації у єдину систему. Облікові фахівці наповнюють цю систему інформаційними ресурсами, а інформаційні агенти (стейкхолдери) отримують та використовують їх для ухвалення управлінських рішень. На кожному з етапів опрацювання облікової інформації на внутрішньому та зовнішньому рівнях обліково-управлінської взаємодії інформаційному середовищу підприємства загрожують кіберзагрози.

Глобальні військові конфлікти, пандемія COVID-19, зростання корупційної складової економіки призвели до активізації кіберризиків у сфері бухгалтерського обліку. Збільшення кількості кібератак як частини гібридних воєн пов’язане з маніпулюванням обліковими даними, їх викривленням та заміною для завдання економічних збитків великим підприємствам і секторам економіки, що призводить в кінцевому випадку до завдання шкоди економічній безпеці країни. Пандемічні зміни

робочого процесу дистанціювали та ізолювали працівників, що вимагало забезпечення активного інформаційного обміну між робочими місцями фахівців та інформаційною базою підприємств-роботодавців. Активне використання комунікаційних сервісів реалізації функціональних обов'язків привернуло увагу кіберзлочинців, метою яких є викрадення комерційної таємниці та інтелектуальної власності підприємства. Аналогічний вплив на облікові процеси мають економічні дисбаланси та корупційні загрози бізнесу, що призводить до значного зменшення витрат на кібербезпеку суб'єктів господарювання. Як наслідок, значно зросла кількість вразливостей системи кіберзахисту бухгалтерського обліку та управління. Варіативність кіберризиків безпосередньо залежить від виду стейкхолдерів. Групування користувачів облікової інформації за різними критеріями для цілей кібербезпеки дає змогу більш ефективно розробляти адекватні методи попередження, уникнення та усунення кібератак.

Базовим критерієм поділу користувачів облікової інформації на внутрішніх та зовнішніх є просторове розміщення стейкхолдерів за причетністю до інформаційного середовища підприємства. Внутрішній персонал і менеджмент підприємств різних рівнів є основним користувачем облікової інформації та модератором управлінських рішень, а тому піддається частим кібератакам. Як проаналізовано у науковій праці [39, с. 87-88], досить часто науковці розглядають інформацію, пов'язану лише з функціонуванням працівників та власників (засновників) підприємства, як об'єкт кіберризиків, тим самим визнають існування лише внутрішніх користувачів облікової інформації у частині кіберзахисту підприємств. Як доводить дослідження EY Global Information Security Survey, особиста інформація персоналу та інформація про власників й менеджерів є основним об'єктом кібератак на підприємствах (17 % та 11 % відповідно). Додатково 34 % суб'єктів господарювання зазнали активних кіберзагроз у зв'язку з недбалістю чи необізнаністю працівників, що є внутрішніми стейкхолдерами (табл. 1.4). А більшість кібератак (38 %), за даними EY Global Information Security Survey, організовані актуальними або звільненими працівниками підприємств [99].

Таблиця 1.4

Об’єкти та вразливості кіберзахисту підприємств

Об’єкт кібератак	**Частка підприємств**	**Вразливості кіберзахисту**	**Частка підприємств**
Особиста інформація персоналу	17 %	Недбалі, необізнані працівники	34 %
Інформація про фінансово-грошові операції	12 %	Застарілий контроль безпеки	26 %
Стратегічні плани	12 %	Несанкціонований доступ сторонніх осіб	13 %
Інформація про власників і менеджерів	11 %	Пов’язані з використанням хмарних обчислень	10 %
Інформація про клієнтів	11 %	Пов’язане зі смартфонами, планшетами	8 %
Інформація про НДДКР	9 %	Пов’язані зі соціальними мережами	5 %
Інформація про злиття та поглинання	8 %	Пов’язані з Інтернетом речей	4 %
Інтелектуальна власність	6 %		
Інформація про постачальників	5 %		

Джерело: сформовано на основі [99]

Проте, облікова інформація, яка стосується зовнішніх фінансово-господарських процесів, все частіше стає об’єктом кібератак в умовах активізації глобальних військових конфліктів та пандемії COVID-19 (інформація про фінансово-грошові операції – 12 % підприємств, інформація про клієнтів – 11 %, інформація про злиття та поглинання – 8 %, інформація про постачальників – 5 %). 13 % суб’єктів господарювання виявили, що кіберзагрози стали можливими через отримання несанкціонованого доступу особами, зовнішніми за відношенням до інформаційної системи підприємства [99]. Як наслідок, винятково внутрішнє позиціонування кіберзахисту є обмеженням його важливої місії у формуванні комплексної системи інформаційної та економічної безпеки підприємства.

У той же час, присутні нечисленні наукові праці, які значно розширюють коло користувачів облікової інформації, що потребують кіберзахисту. Наприклад, Шишкова Н. Л. визначила перелік засобів кіберзахисту у розрізі окремо внутрішніх та зовнішніх користувачів.

Проте, відсутнє пояснення відмінності у забезпеченні кіберзахисту різних груп стейкхолдерів [40, с. 121-122].

Боримська К.П. позиціонує фіскальну службу важливим стейкхолдером облікової інформації, якому загрожують кібератаки. Науковцем пропонується система кіберзахисту, яка передбачає: визначення конфіденційної інформації, удосконалення посадових інструкцій, використання «цифрових підписів» у податкових цілях, застосування програмно-технічних засобів захисту у процесі комунікації з фіскальною службою [4, с.17-18]. Натомість, Rasche A. та Esser D. розробили стандарти захисту інформації окремо для внутрішніх та різних зовнішніх користувачів. Користувачам, на думку науковців, рекомендовано використовувати стандарти при отриманні та опрацюванні облікової інформації для її захисту [148, с.255]. Аналогічної думки Chikutuma C., яка обґрунтувала доцільність формування інтегрованої звітності як дієвого комунікаційного каналу передачі інформації одночасно внутрішнім та зовнішнім стейкхолдерів. Науковцем обґрунтовується потреба безпекового розмежування інформаційних потреб різних груп користувачів для збереження комерційної таємниці та забезпечення кіберзахисту суб'єктів звітування [64]. Продовжив дослідження Шпак В. А., розробивши методику захисту документообігу підприємства у рамках інформаційного обміну з внутрішніми та зовнішніми інформаційними контрагентами. Автором обґрунтовано поняття конфіденційних документів із різним правом доступу до нього стейкхолдерів [41, с.186].

Але, розмежування користувачів за критерієм просторового розташування щодо інформаційного середовища підприємства утруднює ефективне забезпечення кіберзахисту підприємств у зв'язку з можливістю відношення певних стейкхолдерів одночасно до внутрішніх на зовнішніх. Складно розробляти засоби мінімізації кіберзагроз в умовах неможливості чіткої кластеризації суб'єктів безпекових процесів.

Масштабне дослідження наукових позицій щодо варіантів класифікації користувачів облікової інформації провів Чухно І.С. На основі виявлених колізій у традиційній класифікації користувачів на

внутрішніх та зовнішніх автором запропоновано виходити з можливості стейкхолдерів управляти діяльністю господарюючого суб'єкта. Відповідно, науковцем виокремлено три групи користувачів інформації:

1) особи, що приймають управлінські рішення;

2) особи, що не приймають управлінські рішення, але мають фінансову зацікавленість;

3) особи без фінансової зацікавленості [39, с.88].

Поділяючи думку науковця, необхідно зауважити, що поділ стейкхолдерів за критерієм фінансового та управлінського інтересу вирішує проблему їхньої асоціації з внутрішніми або зовнішніми особами. Персонал разом з власниками (засновниками), незалежно від просторового відношення до інформаційного середовища підприємства, можуть бути водночас внутрішніми і зовнішніми стейкхолдерами.

Лаговська О.А., Легенчук С.Ф., Кузь В.І., Кучер С.В. одними з перших класифікують стейкхолдерів облікової інформації для цілей кібербезпеки на користувачів: з повним правом, з обмеженим правом і таких, що використовують вільноприлюднену звітність [112, с.28]. Схожа позиція і у Щирської А. Ю. щодо виокремлення інсайдерів та аутсайдерів як користувачів облікової інформації з наявністю і відсутністю прав доступу до облікової інформації відповідно [42, с.215].

Також El-Ebiary Y. і Alawi N., досліджуючи ризики бухгалтерського обліку як частини інформаційної системи підприємства, визначає необхідність класифікації стейкхолдерів за імовірністю виникнення кіберзагроз. Залежно від актуальності певних кіберзагроз для кожного з трьох видів користувачів (з високою, зі середньою та з низькою ймовірністю) облікової інформації необхідними є варіативні методи забезпечення кіберзахисту [77].

Отже, класичні підходи до класифікації користувачів облікової інформації є недієвими для цілей забезпечення кіберзахисту підприємств. Іншими словами, кіберзагрози можуть не змінюватися для стейкхолдерів у рамках однієї класифікаційної групи.

Основним критерієм поділу користувачів на групи для цілей кібербезпеки підприємств, на що звертають увагу зазначені науковці, є

рівень доступу до облікової інформації. Рівень доступу доцільно трактувати як максимально можливий обсяг та вид облікових даних, які надаються до опрацювання користувачам, враховуючи їхні професійні та поведінкові характеристики. Право отримати облікову інформацію за таких умов безпосередньо пов'язане з можливістю доступу до комерційної таємниці підприємства та випливає від виду обліку (фінансового, управлінського тощо). За цим критерієм доцільно виокремлювати стейкхолдерів з абсолютним доступом, повним доступом, обмеженим доступом і доступом до вільної інформації.

1) Користувачами з абсолютними правами є управлінський персонал з необмеженим рівнем доступу до облікової інформації, яка використовується для перспективного управління підприємством. Такі користувачі використовують максимально наявний масив даних, що формуються управлінським та фінансовим обліком.

2) Користувачі з повними правами мають доступ до конфіденційної інформації за певним напрямом управлінської або фінансово-господарської діяльності підприємства. Наприклад, управлінський персонал використовує облікову інформацію управлінського обліку стратегічного або тактичного характеру для прийняття стратегічних та тактичних управлінських рішень.

3) Користувачам з обмеженим доступом забезпечується право на реалізацію предметно-функціональних дій щодо підприємства, інформація про окремий аспект діяльності якого надається до використання. Зокрема, фіскальні інституції отримують у розпорядження податкову звітність і за потреби подають запит на отримання додаткової облікової інформації у формі первинних та синтетичних документів тощо.

4) Користувачі з вільним доступом не потребують запиту на отримання права на використання облікової інформації. Вони використовують дані, які знаходяться у вільному доступі, публічно оприлюднені. Така облікова інформація не містить конфіденційних відомостей і в основному готується фінансовим обліком.

За можливістю розпоряджатися правом доступу до облікової інформації стейкхолдерів доцільно класифікувати на правонадавачів

(наділяють правом отримувати і розпоряджатися даними) та правоотримувачів (носіїв права інформаційного доступу). Досить часто користувачі інформації можуть належати до обох груп одночасно. Правоотримувач на правах супідрядності може делегувати (передати право доступу) повноваження обробки інформації іншим особам. Наприклад, потенційні інвестори, отримавши облікову інформацію, передають її інвестиційним брокерам. Тому правоотримувач може бути одночасно правонадавачем.

На основі реалізації права доступу до облікової інформації також доцільно виокремити наступні класифікаційні критерії: доступ до облікових об'єктів, функціональні права та порядок обробки інформації. Відповідно до об'єктного спрямування, стейкхолдерам надається право опрацювання інформації винятково про певні об'єкти обліку. Наприклад, фахівцю з грошових розрахунків доцільно надавати дозвіл працювати з функціональним меню комп'ютерних програм для обліку й управління готівкою і банківськими трансакціями. Інші об'єкти обліку залишаються недоступними для вузько-спеціалізованого фахівця. Регламентація функціональних повноважень передбачає обмежену реалізацію функцій обліку: заповнення первинних документів, проведення контрольних процедур, узагальнення облікових даних у регістрах, проведення податкових розрахунків тощо. Стейкхолдерам, залежно від посадових обов'язків, можна заборонити обробку облікової інформації, зокрема: переглядати чи вносити відомості; верифікувати (проводити) дані, змінювати інформацію, яка вступила в дію; вилучати облікові записи; передавати показники на наступні етапи обробки.

Відповідно, користувачів облікової інформації доцільно класифікувати за такими безпековими критеріями: функціональні права (робота з первинними документами, проведення контрольних процедур (у тому числі –інвентаризації), систематизація даних, аналіз показників й прийняття рішень; визначення облікової політики); обробка облікової інформації (внесення, редагування, проведення, узагальнення, передача та архівування даних); об'єкт обліку (необоротні активи, запаси, грошові кошти, дебіторська заборгованість, кредиторська заборгованість, капітал,

заробітна плата, податки і збори, доходи та витрати або більш деталізовані об’єкти). Найчастіше стейкхолдери наділені комбінованими правами. Чим менше підприємство, тим більша концентрація прав у користувача облікової інформації. На невеликих суб’єктах господарювання одна особа може виконувати усі облікові процеси, що передбачає отримання повних прав на оперування інформацією. Фізичні особи – суб’єкти підприємницької діяльності, які одночасно виконують господарські, облікові та управлінські функції, є носіями абсолютних прав, оскільки правонадавач і правоодержувач є однією особою.

Наступною класифікаційною ознакою поділу стейкхолдерів з позиції необхідності забезпечення кіберзахисту є вид економічної діяльності. Стейкхолдери, що є представниками різних видів економічної діяльності, також піддаються варіативним кіберризикам (табл. 1.5). Відповідно, користувачів облікової інформації доцільно групувати за приналежністю до секторів економіки.

Як демонструють дослідження Union Agency for Cybersecurity, у 2023 р. значно зросли кіберзагрози для усіх видів економічної діяльності, що пов’язане з ізоляцією, дистанціалізацією, зростанням інформаційних та фінансових ресурсів на проведення військових дій. Кіберризики для різних секторів економіки можуть повністю відрізнятися, наприклад для домогосподарств – це: фішинг, витік інформації, викрадення даних, а для промисловості – зловмисне програмне забезпечення, атаки веб-додатків, інсайдерська загроза (ненавмисне зловживання) [160].

Вид актуальних кіберзагроз для кожної галузі економіки також залежить від приналежності стейкхолдерів до фізичних чи юридичних осіб. При поділі користувачів облікової інформації на фізичні та юридичні особи необхідно враховувати вікові параметри та організаційно-правову форму відповідно. Для фізичних осіб певного вікового складу притаманні диференційовані кіберзагрози. Різні вікові групи стейкхолдерів характерні особливими поведінковими ознаками, що посилює влив тих чи інших кіберризиків. За критерієм вікової структури стейкхолдерів доцільно ранжувати на групи: молодша (до 35 років) середня (36-50 років), старша (51-65 років) і похила (старше 66 років).

Таблиця 1.5

Актуальність кіберзагроз для різних секторів економіки

Сектор	**Основні загрози**	**Тренд у 2023 р. / 2022 р.**	**Вплив чинників**
Фізичні особи / Домогоспо-дарства	Фішинг Витік інформації Викрадення даних	=	Самоізоляція як спосіб боротьби з COVID-19 сприяла децентралізації ІТ-середовища та ізоляції Інтернет користувачів, які піддаються кіберзагрозам та менше приділяють уваги кібербезпеці.
Промисловість	Зловмисне ПЗ Атаки веб-додатків Інсайдерська загроза (ненавмисне зловживання)	=	Крадіжка облікових даних, що містить комерційну таємницю, є значною загрозою для цього сектору. Також кібератаки на ланцюги поставок та на системи промислового контролю є причиною призупинення виробничого процесу.
Багато-галузевий бізнес	Атаки веб-додатків Фішинг Зловмисне ПЗ	+	Віддалена робота працівників як спосіб боротьби з COVID-19 активізувала фішингові атаки, що загрожуй втраті конфіденційної облікової інформації.
Державне управління, оборона, соціальні послуги	Зловмисне ПЗ Фішинг Веб-атака	+	Використання хмарних сервісів призвело до зростання кіберзагроз адміністративному сектору держави. Соціальні служби зазнали кібератак через сервіси фінансової допомоги громадянам під час пандемії COVID-19 та воєнних дій.
Фінанси / Банківська справа / Страхування	Атаки веб-додатків Інсайдерська загроза (ненавмисне зловживання) Зловмисне ПЗ Викрадення даних	=	Багатоаспектність фінансового сектору економіки ускладнює чітке виокремлення кіберзагроз, оскільки різні сфери фінансових та банківських послуг можуть піддаватися абсолютно різними кіберризиками у сфері бухгалтерського обліку.
Охорона здоров'я / Медицина	Зловмисне ПЗ Інсайдерська загроза (ненавмисна зловживання) Атаки веб-додатків	+	Відбувалася актуалізація кіберзагроз в охороні здоров’я через інтерес шахраїв до інформаційних та фінансових ресурсів, які виділяються на боротьбу з пандемією COVID-19 та військовими загрозами.
Освіта	Зловмисне ПЗ Вимагальна програма Веб-атаки	+	Збільшення активності кібершпигунських кампанії через інтерес до облікових та наукових ресурсів, пов’язаних з дослідженням COVID-19 та воєнних дій.
Інформація та комунікація	Атаки веб-додатків Інсайдерська загроза Зловмисне ПЗ	=	Із зростанням кількості цифрових медіа актуальними стають кіберризики щодо зміни публічної інформації для управління громадською думкою.
Мистецтво, розваги та ігри	Атаки веб-додатків Зловмисне ПЗ Фішинг	=	Перехід від ліцензійної до підписної реалізації творів інтелектуального виробництва ігрової індустрії через Інтернет зробив цей сектор більш привабливим для кіберзлочинців.

Джерело: систематизовано на основі [160]

Молодші користувачі отримують інформацію в основному через соціальні мережі та месенджери, що потребує обмеженого їхнього використання у господарських та управлінських цілях. Середня вікова група найбільш активно серед інших стейкхолдерів користується програмним забезпечення для оперування обліковою інформацією, а також спеціалізованими Інтернет-сторінками. Таким особам переважно загрожують вірусні та хакерські атаки, що потребує використання антивірусних програм. Стейкхолдери із групи старшого віку частіше піддаються фішинговим та спамовим атакам через електронну пошту, а також з використанням платіжних сервісів і банківських карток. Доцільно застосовувати браундмаузери, спам фільтри та системи додаткової верифікації електронних трансакцій. Користувачі похилого віку більше піддатливі до шахрайських дій з використанням телефонів (дзвінки та повідомлення), що потребує використання спеціалізованого програмного забезпечення для фільтрування телефонного трафіку.

Зрозуміло, що виокремлення кіберзагроз для кожної вікової групи є умовним, але водночас наведені ризики – найбільш імовірні й типові для відповідних стейкхолдерів. Користувачі облікової інформації, через вплив вікових та поведінкових характеристик, захищені від одних кіберризиків та піддатливі до інших.

На відміну від вікової структуризації фізичних осіб, для юридичних осіб доцільно застосовувати класифікацію відповідно до їхньої організаційно-правової форми. З метою посилення кібербезпеки юридичних осіб доцільно поділяти на: акціонерні товариства (використовують та обов’язково оприлюднюють значні масиви облікової інформації відповідно до вимог законодавства), господарські товариства (обмежена відповідальність перед контрагентами), державні установи й інституції (носії конфіденційної інформації, що містить державну таємницю), об’єднання підприємств (використовують систему складних перманентних комунікацій між учасниками об’єднання), непідприємницькі утворення (мають значний інформаційний вплив на соціальне, культурне, побутове, релігійне функціонування суспільства).

Кожній групі суб'єктів господарювання притаманні варіативні особливості опрацювання облікової інформації. Залежно від виду організаційно-правової форми, відрізняються і кіберзагрози. Наприклад, державні інституції піддаються значним хакерським атакам з метою викрадення державної таємниці або завдання шкоди національній безпеці. Виокремлення зазначених груп дає змогу ідентифікувати найбільш імовірні кіберризики та виробити превентивні заходи із забезпечення кіберзахисту.

Важливим критерієм класифікації стейкхолдерів щодо доступу до облікової інформації є вид застосовуваних комунікаційних каналів. Більшість сучасних ділових комунікацій реалізуються через мережу Інтернет. Відповідно, користувачів (відправників, одержувачів) облікової інформації доцільно поділяти на осіб, які використовують: електронну пошту (різні поштові сервіси), алгоритми обміну даними між програмними продуктами облікового призначення (наприклад, синхронізація даних 1С: Бухгалтерія та M.E.Doc), соціальні мережі та месенджери (Facebook, VK, Viber, Whatsapp, Telegram тощо), файлообмінники та хмарні сховища (Dropbox, OneDrive, Google Drive та ін.), внутрішню мережу даних (локальну мережу передачі інформації), фізичні носії (паперові документи, флеш-носії, компакт-диски).

Від виду комунікаційного каналу, який традиційно застосовується стейкхолдерами, залежить комплексність контрольних дій. Користувачі облікової інформації, які використовують декілька каналів передачі (отримання) інформації, піддаються більш складним і частим кіберризикам. Інформаційні операції деяких стейкхолдерів, наприклад тих, що використовують соціальні мережі та месенджери, потребують перманентно кіберзахисту. І навпаки, користувачі інформації на фізичних носіях майже не піддають кіберризикам.

Класифікацію стейкхолдерів за видом комунікаційних каналів також доцільно використовувати для обмеження доступу до певних Інтернет-сервісів у процесі реалізації функціональних обов'язків для попередження прояву кіберзагроз. Додатково може існувати загальнонаціональна заборона на використання Інтернет-ресурсів, що можуть загрожувати

кібербезпеці країни. Наприклад, в Україні вимкнутий доступ до соціальних мереж VK, Odnoklasnuku, електронної пошти mail.ru, файлообмінника і пошуковика Yandex, облікового програмного забезпечення 1С : Бухгалтерія та багато інших, застосування яких призводить до потенційної втрати інформації, що містить комерційну і військову таємницю.

Окрім виду комунікаційного каналу, для забезпечення кібербезпеки важливе значення має частота інформаційних актів. Залежно від періодичності подання запитів або отримання облікової інформації зростає імовірність появи кіберзагроз. Тому для оцінки необхідних заходів кіберзахисту доцільно виокремлювати стейкхолдерів з: перманентними (інформаційна синхронізація відбувається на постійний основі), частими (щоденний обмін інформацією), періодичними (передача та отримання інформації відбувається з певною періодичністю: кожного тижня, в кінця місяця чи кварталу тощо) та одиночними комунікаціями (після виникнення потреби в обліковій інформації, наприклад, в інвестора раз в рік для пошуку об’єктів інвестування).

Узагальнена класифікація користувачів облікової інформації відображена у табл. 1.6 за критеріями: можливості управляти діяльністю господарюючого суб’єкта, правом доступу, імовірності появи кіберзагроз, можливості розпоряджатися правом доступу, доступу до облікових об’єктів, функціонального права, порядку обробки інформації, виду економічної діяльності, віку фізичних осіб, організаційно-правової форми юридичних осіб, виду застосовуваних комунікаційних каналів, частоти інформаційних актів.

Окрім запропонованих варіантів поділу стейкхолдерів керівництво підприємства може самостійно доповнювати перелік довільними видами користувачів облікової інформації, що відповідатиме безпековим потребам. Натомість деякі класифікаційні критерії, як от кількість штатних працівників чи обсяг прибутку, які є визначальними при виокремленні різних видів суб’єктів господарювання, не впливають на імовірність появи тих чи інших кіберризиків.

Таблиця 1.6

Класифікація стейкхолдерів облікової інформації з метою забезпечення кібербезпеки підприємств

№ з/п	**Класифікаційний критерій**	**Вид стейкхолдера**
1.	Вид економічної діяльності	Фізичні особи / Домогосподарства; Промисловість; Багатогалузевий бізнес; Державне управління, оборона, соціальні послуги; Фінанси / Банківська справа / Страхування; Охорона здоров'я / Медицина; Освіта; Інформація та комунікація; Мистецтво, розваги та ігри
2.	Можливість управляти діяльністю господарюючого суб'єкта	Приймають управлінські рішення; Особи, що не приймають управлінські рішення, але мають фінансову зацікавленість; Особи без фінансової зацікавленості
3.	Право доступу до облікової інформації	З абсолютними правами; З повними правами; З обмеженими доступом; З вільним доступом
4.	Імовірність появи кіберзагроз	З високою ймовірністю; Зі середньою ймовірністю; З низькою ймовірністю
5.	Можливість розпоряджатися правом доступу	Правонадавач; Правоодержувач
6.	Доступ до облікових об'єктів	З правом доступу до інформації про: Необоротні активи; Запаси; Грошові кошти; Дебіторська заборгованість; Кредиторська заборгованість; Капітал; Заробітна плата; Податки і збори; Доходи та витрати; Більш деталізовані об'єкти
7.	Функціональне право	З правом на: Роботу з первинними документами; Проведення контрольних процедур; Систематизацію даних; Аналіз показників й прийняття рішень; Визначення облікової політики
8.	Порядок обробки інформації	З правом на: Внесення даних; Редагування даних; Проведення даних, Узагальнення даних, Передачу та архівування даних
9.	Вік фізичної особи	Молодша вікова група; Середня вікова група; Старша вікова група; Похила вікова група
10.	Організаційно-правова форма юридичної особи	Акціонерні товариства; Господарські товариства; Державні установи й інституції; Об'єднання підприємств; Непідприємницькі утворення
11.	Вид застосовуваних комунікаційних каналів	Що використовують: Електронну пошту; Алгоритми обміну даними між програмними продуктами облікового призначення; Соціальні мережі та месенджери; Файлообмінники та хмарні сховища; Внутрішню мережу даних; Фізичні носії
12.	Частота інформаційних актів	З перманентними; З частими; З періодичними; З одиночними

Джерело: розроблено автором

В умовах формування цифрової економіки суб’єкти господарювання реалізують господарську діяльність з мінімальним залученням людських ресурсів. Інформаційно-господарські процеси на підприємствах електронного бізнесу значною мірою автоматизовані, а тому кількість працівників не впливає на прояв кіберзагроз та прибутковість бізнесу. Обсяг прибутку також не визначає імовірність появи кіберзагроз. Необхідність забезпечення кібербезпеки аналогічна для комерційних, державних, комунальних чи громадських інституцій. Тому окрема класифікація стейкхолдерів за рівнем прибутковості є недоцільною для організації інформаційного захисту.

РОЗДІЛ 2. УДОСКОНАЛЕННЯ МЕТОДИКИ ОБЛІКУ ДЛЯ ЦІЛЕЙ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВ

2.1. Відкритий документообіг на основі технології блокчейн для кіберзахисту підприємства

З метою забезпечення кібербезпеки керівництво підприємств незалежно від розміру бізнесу вдається до ізоляції конфіденційної інформації від інших інформаційних потоків. Корпоративні об'єднання створюють окрему службу конфіденційного документообігу. Для цієї мети використовують спеціалізоване програмне забезпечення обробки, руху та зберігання конфіденційних документів ізольовано від системи загального документообігу. Працівникам, які оперують інформацією, що містить комерційну таємницю, забороняється використання носіїв інформації та мережі Інтернет в особистих цілях на робочому місці. Вводяться часові та змістові регламенти обробки інформації. Зокрема, регламентується час доступу та змістове наповнення інформації, доступ до якої необхідно обмежити.

Окрім наведених підходів щодо кіберзахисту інформації захищений документообіг, як доводить Шпак В.А., базується на виконанні додаткових правил:

– особистої відповідальності співробітників за збереження носія і таємницю інформації;

– обмеження ділової необхідності доступу персоналу до документів, справ і баз даних;

– жорсткій регламентації порядку роботи з документами, справами і базами даних для всіх категорій персоналу [41].

Проте, ізоляційний підхід до документування та документообігу не гарантує ефективного кіберзахисту підприємства. Відокремлені бази облікових даних привертають підвищену увагу кіберзлочинців. Також завжди присутній інсайдерський вплив на кіберзахист, що реалізується через можливе вербування працівників третіми особами. Внутрішні особи

із правами доступу до конфіденційної інформації можуть її передавати кіберзлочинцям. Іншим варіантом є таємне вбудовування штатними посадовими особами шкідливого програмного забезпечення у систему конфіденційного документообігу з метою інформаційного шпіонажу. Як наслідок, виникають кіберзагрози ізоляційним інформаційним потокам підприємств. Тому для забезпечення ефективної кібербезпеки необхідним є розробка нових форматів організації документування й документообігу.

Науковцями досліджено різносторонні аспекти використання технології блокчейн в бухгалтерському обліку. Наприклад, Bansal S.K., Batra R., Jain N. [57] та Bonson E., Bednarova M. [60] дослідили перспективні тренди у розвитку обліку; O'Leary D.E. – архітектуру технології з визначенням потоків облікової інформації [139]; методику управлінського обліку на різних рівнях управління [139]; Rındasu S.M. – переваги і загрози для обліку [149]; Cai C.W. – можливості впровадження потрійного облікового запису [62]; Coyne J.G. і McMickle P.L. – подолання організаційних перешкод в обліку [66]; Sarkar S. – трансформацію знань, вмінь та професійних навичок облікових фахівців [156]; Karajovic M., Kim H.M. і Laskowski M. – новий спосіб структурування облікової інформації [102]; Sheldon M.D. [163] і Sinha S. [165] – загрози обліковій процесії; Kokina J., Mancha R. і Pachamanova D. – загрози для бухгалтерського обліку [107].

Також проводяться дослідження щодо застосування технології блокчейн для удосконалення інформаційних систем, що інформаційно пов'язані з обліком: Schmitz J. та Leoni G. – перспективи розвитку аудиту та інших видів контролю [159]; Kozlowski S. – перманентний аудит з формуванням контрольної екосистеми підприємства [108]; Liu M., Wu K. і Xu J. – синергетичний взаємозв'язок обліку та аудиту [116]; Gomaa A.A., Gomaa M.I. і Stampone A. – імплементація ERP систем та роль облікової інформації в управлінні підприємством [88]; Tan B.S. та Low K.Y. – формування баз даних для цілей різних груп користувачів [178]; Wu J., Xiong F. і Li C. – взаємозв'язок з іншими видами комп'ютерно-комунікаційних технології для варіативних інформаційних користувачів [187] та інші науковці.

У науковому просторі присутні узагальнюючі та оглядові праці, що стосуються застосування технології блокчейн у бухгалтерському обліку. Зокрема, Pimentel E. та Bouliann E. визначили сім основних напрямків реалізації можливостей блокчейн структурування облікової інформації: майбутнє бухгалтерського обліку, облікові функції, аудит та контрольні процедури, відображення криптоактивів у звітності підприємства, навчання облікових фахівців, адміністративне урядування, оподаткування. Науковці резюмують необхідність встановлення паритету між теоретичними дослідженнями та практичними розробками щодо імплементації технології блокчейн у бухгалтерський облік [143].

Alsaqa Zeyad Hashim, Hussein Ali Ibrahim та Mohammed Mahmood Saddam сформували висновок, що використання технології блокчейн кардинально змінює інформаційну систему обліку на підприємстві. Іншими словами, використання принципів ланцюгово-блокового структурування облікової інформації неможливе в традиційній обліковій системі, а потребує кардинального удосконалення методики, методології та організації бухгалтерського обліку [52].

Tiron Tudor Adriana, Deliu Delia, Farcane Nicoleta та Donțu Adelina дослідили основні перешкоди до впровадження технології блокчейн у бухгалтерських та аудиторських організаціях. Науковцями визначено неготовність підприємств до інновацій як основне організаційне обмеження використання інноваційних технологій та сформовано методику SWOT-аналізу використання технології блокчейн для різних облікових та аудиторських організацій. Також визначено сім перспективних напрямків наукових пошуків щодо впровадження технології блокчейн в облікову практику: забезпечення інформаційної трансперентності та доступності; формування старт-контрактів між учасниками договірних відносин; участь облікових фахівців у формуванні екосистеми блокчейн; оптимізація щоденного функціонування облікових працівників; забезпечення навчання та перенавчання щодо діяльності з інноваційними технологіями; трансформація облікових та аудиторських професій; інституційні зміни та удосконалення нормативно-правового забезпечення [180].

Активізація наукових пошуків щодо особливостей використання технології блокчейн для облікових цілей відбулася у 2018 році. Найбільшої актуальності набули дослідження щодо реалізації облікових та аудиторських функцій в умовах блоково-ланцьового структурування інформації. Непопулярними дослідницькими об'єктами виявилася проблематика формування первинних й звітних документів та навчання й перенавчання облікових фахівців в умовах імплементації новітніх комп'ютерно-комунікаційних технологій. Піком активності формування глобальної наукової думки про обліковий аспект імплементації технології блокчейн став 2021 рік, що пояснюється значною публічною увагою до криптографічних активів (рис. 2.1).

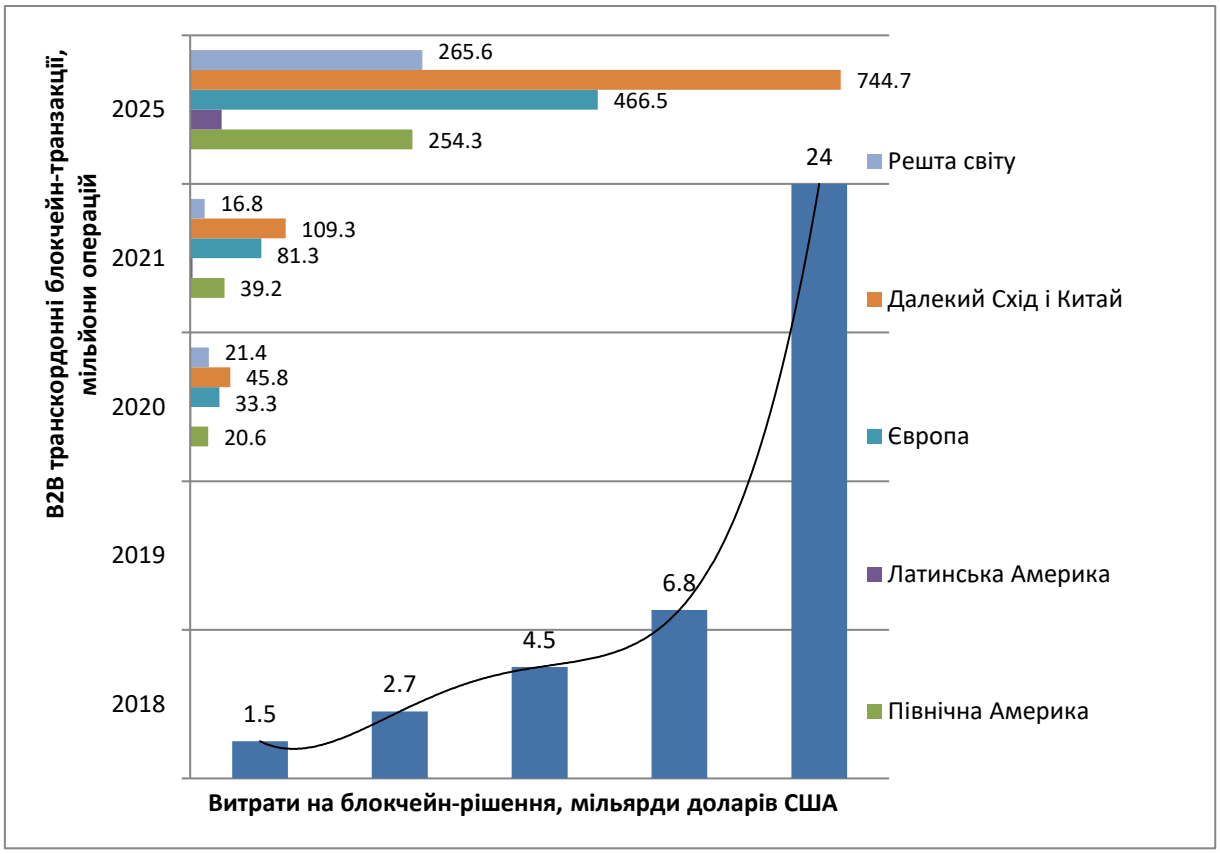


Рис. 2.1. Популяризація технології блокчейн у 2018-2025 рр.

Джерело: сформовано на основі [186]

Як очікується у 2021 році обсяг інвестицій у технологію блокчейн зросте з 4,5 мільярди доларів США до 6,8 мільярди доларів США, а у 2025 році – становитиме уже 24 мільярди доларів США. Кількість інформаційних операцій з використанням принципів блоково-ланцюгового структурування інформації збільшується у кожному з географічних регіонів. Лідерами з впровадження технології блокчейн є країни далекого Сходу та Китаю і Європи, що підтверджується й національною приналежністю дослідників проблематики блоково-ланцюгового структурування інформації.

Проте науковцями у галузі бухгалтерського обліку і пов'язаних з ним науково-прикладних сфер приділена неналежна увага можливостям використання технології блокчейн для забезпечення кіберзахисту облікової інформації. Узагальнюючи напрацювання науковців у сфері використання технології блокчейн, можливо систематизувати її фундаментальні принципи з позиціонування можливості кіберзахисту інформації у табл. 1.

При науковому пошуку перспектив забезпечення кіберзахисту підприємств на основі використання технології блокчейн у бухгалтерському обліку необхідно орієнтуватися на її фундаментальні принципи: фрагментованість, взаємне доповнення, масштабованість, дублювання, хронологічність, конфіденційність, розподіленість, доступність, відкритість обробки облікової інформації.

Більшість документів в інформаційному кругообігу підприємств є облікового походження. Бухгалтерський облік генерує первинну економічну інформацію. Документування господарських процесів і явищ є первинним елементом методу бухгалтерського обліку. Тому економічні дані, зібрані й задокументовані, носять назву «первинні». Первинне документування є початковим етапом обробки облікової інформації. Від достовірності та надійності інформації, що містяться у первинних документах, залежить кіберзахист усієї інформаційної системи підприємства.

Таблиця 1

Принципи технології блокчейн у частині забезпечення кібербезпеки облікової інформації

№ з/п	Фундаментальний принцип	Реалізація для цілей кібербезпеки облікової інформації
1.	Фрагментованість	Поділ облікової інформації на окремі фрагменти (блоки), які окремо не мають цінності для кіберзловмисників
2.	Взаємне доповнення	Кожний блок через ланцюгове поєднання доповнює інші блоки інформації. При створенні нового блоку дані про нього вноситься в усі інші пов'язані блоки, що запобігає фіктивній появі нової облікової інформації
3.	Масштабованість	Нові блоки та модулі можуть додаватися до бази даних без обмежень, що сприяє використанню єдиних систем кіберзахисту облікової інформації на усіх підприємствах незалежно від розміру бізнесу, організаційно-правової форми чи інших організаційних чинників
4.	Дублювання	Кожний блок може дублюватися в інших місцях зберігання, що дає змогу відновлювати випадково втрачену або знищену облікову інформацію
5.	Хронологічність	Ведеться хронологічний перелік змін облікової інформації, що дає змогу виявляти несанкціоновані дії, що призвели до відхилення від еталонного зразка
6.	Конфіденційність	Усі операції з обробки облікової інформації здійснюються поза офіційними чи урядовими сервісами, що унеможливлює контроль та відслідковування дій облікових чи управлінських фахівців
7.	Розподіленість	Облікова інформація розміщується у розподіленій базі даних, у якій кожний з фрагментів може зберігатися на багатьох напряму не пов'язаних технічних пристроях, що не є власністю підприємства. Унеможливлюються кіберзагрози програмному й технічному забезпеченню.
8.	Доступність	Облікова інформація розміщується у загальнодоступних хмарних базах даних, що запобігає блокуванню кіберзлочинцями доступу
9.	Відкритість	Технологія є відкритою до застосування, що робить її популярною у фінансовій, комерційній, фіскальній, адміністративній та, що особливо важливо, безпековій сфері

Джерело: сформовано автором

Кіберзагрози паперовому документуванню і документообігу традиційно позиціонувалися як внутрішні зловмисні маніпуляції працівниками підприємства або випадкові помилки. Іншим джерелом зовнішнього надходження недостовірних документів є контрагенти підприємства, які можуть змінювати облікові дані з метою певного економічного зиску. Натомість, в умовах переходу на електронне

документування та документообіг активізуються зовнішні кіберзагрози підприємства. Первинні облікові дані стають цінним інформаційним ресурсом та, відповідно, об'єктом кібератак.

За традиційного документообігу з елементами ізольованості облікової інформації обов'язковим є регламентація шляху документа від відправника до адресата. Потенційні одержувачі облікових даних формують інформаційні запити і направляють їх до бази даних. Зі загального інформаційного масиву здійснюється вибірка показників, які є корисними та потрібними для певного виду стейкхолдерів. Для забезпечення кіберзахисту важливим є обмеження доступу до конфіденційних документів. Дозування облікової інформації відбувається через систему фільтрів, які відбирають та блокують документи на шляху до одержувача. Тобто, стейкхолдер отримує інформацію відповідно до інформаційних запитів та права доступу. Ініціатором інформаційного процесу в умовах традиційного документообігу на підприємстві є користувачі облікової інформації, що шкодить своєчасності та безпеці обліку.

Натомість організація документообігу на основі технології блокчейн мінімізує потребу у регламентації інформаційних потоків. Факт виникнення фінансово-господарського явища чи події та його відображення в первинних документах запускає подальший інформаційний процес. На основі вивчення інформаційних уподобань стейкхолдерів, ідентифікації права доступу до комерційної таємниці, посадових інструкцій, автоматизована система управління здатна кластеризувати та розподіляти інформацію. Задукоментований масив облікових даних в момент його виникнення та фіксації в обліковій системі може автоматично направляється до цільового користувача.

Облікова інформація оперативно надходить до стейкхолдера, який відповідальний за її обробку або потребує повного інформаційного ресурсу для своєчасного прийняття управлінських рішень. Оптимізуються часові критерії обробки облікової інформації. На відміну від традиційного документообігу задокументовані дані з невеликим часовим лагом одномоментно передаються для подальшої обробки чи споживання. У

системі електронного документообігу доцільно передбачити методику контролю зворотних реакцій на отриману стейкхолдерами облікову інформацію. Необхідний контроль факту одержання користувачем первинних даних, їхнього опрацювання посадовими особами, наявності відповідного управлінського рішення щодо коригування діяльності суб'єкта господарювання тощо. При контролі зворотного зв'язку унеможливлюються помилки; інформаційне дублювання; перенасичення чи недостача облікової інформації та, основне, цілеспрямовані кібератаки на систему обліку підприємства.

За допомогою технології блокчейн облікова інформація фрагментується на численні складові, які можуть дублюватися із накопиченням у різних блоках та доповнюватися для майбутнього об'єднання у єдину сукупність. Кожний інформаційний фрагмент може зберігатися на різних технічних пристроях чи хмарних сервісах обробки інформації. З використанням методики блокчейн структурування інформації зникає потреба у додаткових засобах кіберзахисту підприємства.

Кібербезпека підприємства на основі технології блокчейн реалізується через фрагментацію та випадковий розподіл облікової інформації одразу в момент її документування. Після збору первинні дані дробляться на окремі інформаційні масиви, напряму непов'язані між собою. Додатково можливе шифрування інформації та запис в розподілене хмарне середовище. Кожний фрагмент облікових даних не несе змістового навантаження. Лише у кінцевого користувача елементи облікової інформації інтегруються в єдину інформаційну модель, що може бути корисною та цінною для подальшого використання. Фрагментована облікова інформація може бути відкритою, оскільки без наступного об'єднання не має інформаційної цінності для кіберзлочинців. Зменшується необхідність в організації ізольованих систем документообігу, оскільки розподілена облікова інформація перебуває під надійним інформаційним захистом.

Через використання технології блокчейн реалізується надійний безпековий захист перш за все бізнес-комунікацій. Документальний

супровід ділових взаємовідносин потребує ефективного кіберзахисту з метою унеможливлення прояву кіберзагроз. Внесені контрагентом документи необхідно фрагментувати й шифрувати при внесені до єдиної бази даних. Законтрактовані у документах договірні відносини захищені від стороннього видозмінення. Також унеможливлені необумовлені зміни й сторонами ділових взаємовідносин. Контроль виконання договірних зобов'язань доцільно здійснювати на основі моніторингу первинних документів з реалізації матеріальних цінностей (робіт, послуг) та грошових транзакцій.

Для реалізації кіберзахисту облікової інформації між контрагентами за спільного погодження доцільно використовувати єдиний сервіс хмарного документообігу. Іншими словами, усі учасники договірних відносин обирають Інтернет платформу для спільного документообігу щодо оформлення та виконання комерційний угод. Хмарні сервіси документообігу доцільно інтегрувати у внутрішні інформаційні системи підприємств. Як наслідок, вихідне оформлення або вхідне отримання електронних примірників документів одночасно фіксується у двох базах даних: кожного підприємства та інформаційного об'єднання підприємств-контрагентів. Перспективним в умовах становлення цифрової економіки є також інформаційна інтеграція усіх контрагентів в єдину базу електронного документообігу на основі технології блокчейн.

За допомогою технології блокчейн виявляються масиви інформації, які були об'єктом внутрішніх або зовнішніх кібератак. Наприклад, на основі моніторингу історії змін певних документів та їхнього порівняння з еталонними зразками доцільно ідентифікувати осіб – порушників інформаційного режиму. Натомість факт появи зовнішніх несанкціонованих змін в інформаційному середовищі підприємства, які відрізняються від аналогічних інформаційних масивів з інших джерел, може бути свідченням кібервтручання. Виявлений інцидент, що відбувався з порушенням часового, інформаційного та правового регламенту, доцільно розцінювати як кібератаку. У випадку втрати, викривлення або знищення зловмисниками інформаційних фрагментів можливе їхнє автоматичне відновлення з розподіленої бази даних.

Ланцюгово-блокове структурування облікової інформації спрощує процес архівного зберігання документів. Розподілену базу облікових даних доцільно розміщувати в мережі взаємопов'язаних хмарних сервісів, що забезпечує доступність архівної інформації для користувачів. Хмарне архівування електронних документів на мережі взаємопов'язаних серверів гарантує їхнє збереження, цілодобовий доступ та кіберзахист. На вимогу стейкхолдерів розрізнені масиви архівної облікової інформації вилучаються з електронних архівів та рекомбінуються для відображення документа у традиційній формі як сукупності певних реквізитів. Такими стейкхолдерами можуть бути як внутрішні користувачі інформації (облікові чи управлінські фахівців), так і зовнішні – контролюючі чи фіскальні інституції.

Для отримання доступу до електронних документів використовується система цифрових підписів, яка уже активно використовується у фіскальних цілях та отриманні різних державних адміністративних послуг. Застосування електронних ключів має відбуватися на двох етапах: формуванні первинних документів та їхньому відновлені з розподіленої бази даних. Після збору облікових даних доцільно накладати цифровий підпис особами, відповідальними за формування первинних документів, що забезпечує контроль інформаційного авторства. Надалі відбувається фрагментація та шифрування облікової інформації, яка після потрапляння до цільового споживача рекомбінується до початкової форми.

Запропонована інформаційна схема відкритого документообігу на основі технології блокчейн відображена на рис. 2.2.

Для отримання доступу користувач відновленої інформації також використовує персоніфікований цифровий підпис, що є свідченням факту інформаційної обробки чи споживання. Система розподіленого електронного документообігу ідентифікує особу користувача, час доступу та усі зміни облікової інформації, що є важливим елементом кіберзахисту підприємства.

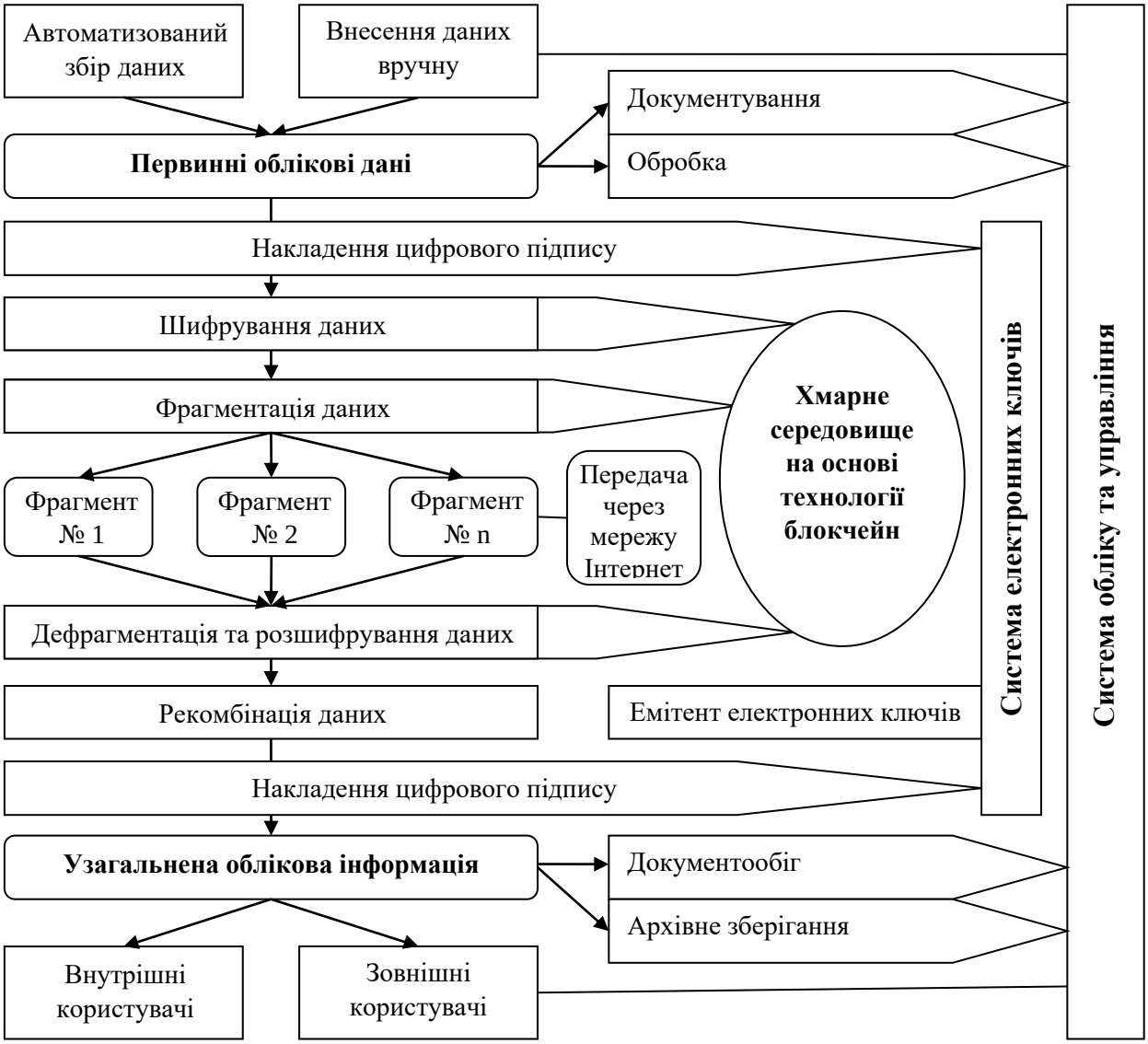


Рис. 2.2. Інформаційна схема відкритого документообігу на основі технології блокчейн

Джерело: сформовано автором

Права доступу стейкхолдерів до бази облікових даних доцільно обмежувати через встановлення терміну дії електронних ключів. Необхідність організації кіберзахисту спонукає до частої зміни цифрового підпису персоналу. Необхідність перевипуску цифрових підписів стимулює стейкхолдерів до оновлення безпекової дисципліни. Кожний користувач змушений звертатися до емітента щодо отримання нового електронного ключа, що сприяє перманентному контролі та перевірці стейкхолдерів. У керівництва підприємства з'являється дієва методика контролю за правомірністю використання електронних форматів

верифікації особи, яка намагається отримати доступ до конфіденційної інформації. Через використання системи електронних ключів користувачі отримують доступ до дозованого обсягу інформації у межах відкритого документообігу.

Реалізація електронного документування та документообігу на базі принципів відкритості даних з використанням технології блокчейн є основною організації кіберзахисту на усіх підприємствах незалежно від форми власності, розміру бізнесу і т.д. Відмова від ізоляційних практик в організації інформаційного обміну у бізнес-середовищі підприємств є елементом формування відкритої національної економіки. Кругообіг облікової інформації в умовах ефективного кіберзахисту на внутрішньому та зовнішньому рівні є стимулом до подальшого розвитку нових технологій у фінансово-господарській сфері («фінтех галузі» економіки). Подальша імплементація комп'ютерно-комунікаційних технологій з виробленням дієвих методів кіберзахисту інформації сприяє уникненню перешкод до подальшого розвитку цифрової економіки та інформаційного суспільства. Як наслідок, організація документообігу з використанням технології блокчейн з метою кіберзахисту обліку сприяє новому інноваційному етапу розвитку суспільної формації.

2.2. Облік та кіберзахист електронних трансакцій з використанням криптовалют

Поступальний розвиток електронних грошових засобів призвів до появи цифрової готівки, активність використання якої пов'язана із зростанням обсягу електронних трансакцій за товари (роботи, послуги), реалізовані через мережу Інтернет. Новітньою тенденцією в розвитку технологій електронних трансакцій є виникнення криптовалют, обіг яких відбувається через телекомунікаційні зв'язки між персональними електронними гаманцями платників до одержувачів коштів [43].

Технологія криптовалют заснована на системі комунікаційних

зв'язків блокчейн, яка є об'єднанням публічних регістрів з накопичення інформації про грошові трансакції. Цілісність блокчейн реалізується через дублювання певного обсягу інформації в кожного користувача системи електронних платежів. Іншими словами, не існує спільного сховища даних, єдиного сервера, на якому акумулюється вся інформації. Тому втрачена частини інформації в одного власника цифрової готівка компенсується за рахунок інших власників електронних гаманців.

Криптовалюти характеризуються повною конфіденційністю, відсутністю централізованого контролю з боку держави та єдиного емітента, що суттєво відрізняє їх від інших електронних платіжних систем. Ці характеристики сприяють використанню криптовалют зловмисниками при реалізації кібератак. Криптовалюту приймають програмами-вимагачі та кібертерористи. За допомогою криптовалют відбувається легалізація коштів, отриманих злочинним способом. Тому використання криптовалют як нового конфіденційного виду електронних грошей неодмінно супроводжуватиметься кіберризиками. Активізацію кіберзагроз у сфері обігу криптовалют можливо продемонструвати на прикладі статистичних даних (рис. 2.3).

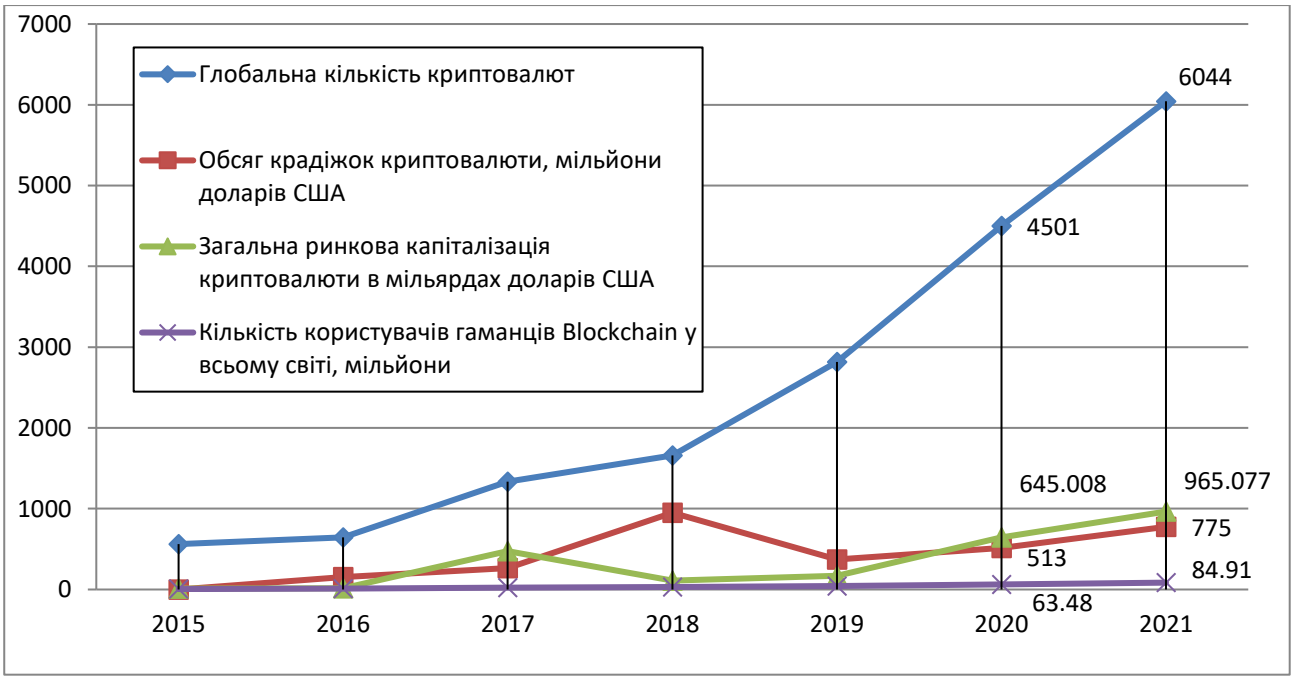


Рис. 2.3. Тренди розвитку ринку криптовалют

Джерело: [78; 137; 138; 182]

Щороку кількість видів криптовалют значно збільшується у глобальному масштабі. Разом зі зростанням ринкової капіталізації криптовалют, починаючи з 2016 року, збільшується кількість крадіжок та інших кіберзагроз у сфері обігу криптоактивів. У 2023 році вартісний вимір кібершахрайства оцінюється у 965 мільйонів дол. США. А у 2018 році цей показник набув пікового значення у майже 1 млрд дол. США.

Зі зростанням обігу криптовалют збільшується кількість науковців, предметом науково-прикладного пошуку яких є криптоактиви. Проте, наукові пропозиції сформовані у більшості випадків за формальними ознаками електронних грошей і пов'язані з усуненням недоліків застосування криптовалют, що є загрозою кібербезпеці підприємств. Поза увагою залишаються особливості використання криптовалют для забезпечення кібербезпеки підприємств. Перспективним є комплексне дослідження обліку та кіберзахисту електронних трансакцій з виокремленням криптовалюти як окремого об'єкта, який докорінно змінює процес електронних взаєморозрахунків та є чинником забезпечення кібербезпеки підприємств.

Функціонування криптобірж та систем грошових трансакцій відбувається на основі використання електронних комунікаційних каналів передачі облікових даних. Актуальними тенденціями в забезпеченні управління безготівковими розрахунками є застосування систем «Інтернет-банк» та «Клієнт-банк», які використовують комунікаційні зв'язки для надання інформації про стан рахунку та дозволу на виконання трансакцій. Основні відмінності двох систем полягають в необхідності використання спеціального програмного забезпечення («Клієнт-банк») та / чи веб-сторінки із доступом до Інтернет мережі («Інтернет-банк») для обміну інформацією.

Недоліком банкінгу через мережу Інтернет є функціональна обмеженість такого варіанту управління рахунком унаслідок збереження усієї облікової інформації в банківській установі та можливість роботи лише в режимі он-лайн. Інтернет-банкінг застосовується в основному фізичними та юридичними особами із незначним грошовим обігом, яким потрібна періодична інформація про стан рахунку. Також інформація із

системи «Інтернет-банк» не може використовуватися для подальшого виконання контрольних та облікових процедур унаслідок її несумісності з програмним забезпеченням підприємств.

Банківським комунікаціям «Інтернет-банк» загрожують активні кіберризики, пов'язаних з функціонуванням мережі Інтернет. Перш за все, зловмисниками може бути заблокований доступ до глобальної мережі через публічні комунікаційні канали. Досить часто зловмисники створюють клони сайтів Інтернет-банкінгу. На таких сайтах відбувається перехоплення інформації з метою отримання персоналізованих даних, що використовуються для доступу до банківських рахунків. Моніторинг даних відбувається через паралельну переадресацію усіх грошових трансакцій на сторонні сервери. В подальшому такі дані застосовуються правопорушниками для викрадення грошових коштів з банківських рахунків. Можливим є перегляд історії грошових трансакцій для встановлення обсягів та одержувачів (відправників) безготівкових платежів, що дає змогу зловмисникам ідентифікувати контрагентів підприємства та дотримання платіжної дисципліни. Тому інформаційний обмін через комунікаційний канал «Інтернет-банк» є ненадійний з позиції забезпечення кіберзахисту.

Дещо більший кіберзахист облікових даних забезпечують банківські комунікації «Клієнт-Банк». Сучасні програмні продукти для автоматизації обліку підтримують систему «Клієнт-Банк» для завантаження виписок з банку та відправлення платіжних документів в електронному вигляді. Але універсальне програмне забезпечення не здатне врахувати індивідуальні особливості технологій комунікацій різних банківських установ та емітентів електронних грошей, що унеможливлює їх вільне використання. Також недоліком системи «Клієнт-Банк» є: відсутність права власності на програмне забезпечення, що встановлюється на робоче місце бухгалтера; можлива несумісність системи «Клієнт-Банк» з іншим програмним забезпечення на підприємстві; відсутність мобільності використання системи (програмне забезпечення встановлюється на один або два комп'ютери облікового персоналу, що створює обмеження щодо використання системи через мобільні пристрої та гаджети); необхідність

присутності усіх осіб, що повинні підписати платіжний документ, в одному місці з персональними комп'ютерами, на яких встановлено програмне забезпечення; значні витрати на інсталяцію необхідного програмного забезпечення та подальшого обслуговування банківською установою системи дистанційного банкінгу [10, с.49-50].

Значною загрозою функціонування програмного забезпечення, що функціонує на принципах технології «Клієнт-банк», є інтродукція в програмний код шкідливих троянських вірусів. Інфікування може відбутися у момент оновлення програмного забезпечення, під'єднання до бази даних банківської (фінансової) установи. Якщо база даних програмного забезпечення «Клієнт-банк» зберігається не на хмарних чи віртуальних серверах, а в локальній мережі підприємства, існує імовірність втрати (пошкодження) облікової інформації.

Також зловмисники, скориставшись періодичною (інколи один раз в день) синхронізацією даних між програмним забезпеченням «Клієнт-банк» та базою даних банківської (фінансової) установи, здатні викривляти облікові показники щодо стану і руху грошових коштів з метою дезінформування керівництва підприємства. Використання недостовірної облікової інформації може призвести до помилкової передачі грошових коштів стороннім особам або прийняття хибних управлінських рішень.

Новим видом кіберзагроз, пов'язаних з використанням шкідливого програмного забезпечення у сфері електронних грошей, є криптоджекінг (незаконний майнінг). Прихований майнінг криптовалют – тип кібератаки через незаконне використання технічного та програмного забезпечення без згоди власників. Банківські, а особливо інші фінансові установи, розповсюджуючи користувацьке програмне забезпечення «Клієнт-банк», можуть використовувати його для криптоджекінгу. Незаконний майнінг складно виявити, а тому краще уникати інсталяцій програмного забезпечення від невідомих фінансових інституцій.

Отже комунікаційні технології «Інтернет-банк» та «Клієнт-банк» не можуть бути ефективними для забезпечення належного кіберзахисту й організації інформаційного обміну між системами обігу критовалюти та

їхнього обліку на підприємстві. Феномен криптовалют ґрунтується на технології блокчейн, реалізація якої передбачає об'єднання усіх власників електронних грошей через мережу комунікаційних каналів, що не потребує наявності єдиного центру опрацювання та накопичення даних.

Об'єднання функціональних переваг технології блокчейн, позитивних якостей комунікацій «Інтернет-банк» та «Клієнт-банк» дозволить створити гібридну систему безготівкових платежів криптовалютами, електронними грошима, коштами на рахунках в банку через платіжні картки та можливості ефективного кіберзахисту інформаційного обміну з усіма учасниками розрахункових операцій (надалі – гібридна система). Гібридну систему доцільно будувати на основі технології блокчейн, що дає змогу уникнути багатьох кіберризиків, притаманних банківським комунікаціям «Інтернет-банк» та «Клієнт-банк».

Функціонування гібридної системи потребує оприлюднення вихідного коду програмного забезпечення на принципах технології блокчейн для публічного ознайомлення. Аналогічно для всіх електронних грошей необхідно забезпечити вільний доступ до універсального програмного модуля безготівкових розрахунків.

Багато емітентів електронних грошей уже надають безкоштовні додатки «Інтернет-банкінгу», які можна вбудувати на веб-сторінку для прийому платежів. Для покупців появляється зручний механізм безготівкових розрахунків за товари і послуги, куплені через мережу Інтернет. Гібридизація реалізовується також завдяки вільній конвертованості усіх існуючих грошових засобів. Будь-яку криптовалюту можна придбати за електронні гроші чи кошти на рахунках в банку. Процес є також зворотним, одержання від платника цифрової готівки передбачає можливість її переведення на рахунок в банку та одержання готівкою у мережі банкоматів.

Проте інтеграція платіжних систем на принципах блокчейн повинна здійснюватися і в напрямку надання інформації про грошові трансакцій в бухгалтерське програмне забезпечення для забезпечення кіберзахисту. Розробники комп'ютерних програм для автоматизації обліку зможуть вбудовувати гібридну систему в програмне забезпечення універсального

чи індивідуального застосування.

Через інформаційну інтеграцію системи електронних платежів в бухгалтерське програмне забезпечення вирішується проблема визнання права власності на комп'ютерну програму, а також повністю ліквідується інформаційна несумісність в організації управління підприємством. Автоматизація обліку безготівкових операцій відбувається в поєднанні з іншими напрямками облікової роботи в єдиному програмному комплексі. Рекомендовано помістити гібридну систему в основу автоматизованого обліку грошових коштів з наданням доступу до безготівкових трансакцій відповідальним особам, забезпеченням дистанційності в управлінні грошовими засобами, організацією ефективного кіберзахисту та контролю з боку менеджменту підприємства й громадськості щодо доцільності грошових операцій тощо.

Завдяки гібридній системі вирішується основний недолік комунікаційної технологій «Клієнт-банк», пов'язаної із неможливістю загального використання програми на багатьох робочих місцях фахівців з обліку та управління. Усім працівникам підприємства, діяльність яких пов'язана з грошовими операціями, рекомендовано надавати доступ до облікової інформації про надходження коштів на поточний рахунок. Наприклад, у місцях реалізації товару працівникам корисно мати інформацію про попереднє надходження коштів від покупця, що дозволить ініціювати видачу замовлення. Розподіл доступу до системи грошових трансакцій та облікової інформації доцільно здійснювати на основі персональних цифрових підписів (логінів і паролів) залежно від позиціонування працівника у ієрархічній структурі управління.

Більш узагальнені дані рекомендовано надавати керівникам різних ієрархічних рівнів на основі Інтернет-доступу та дозволити виконання маніпуляцій через веб-браузер з довільного робочого місця. Будучи територіально віддаленим від самого підприємства чи місця виконання переказу, менеджер та бухгалтер зможе здійснювати моніторинг процесу виконання трансакції через власний мобільний пристрій. Також за менеджерами різних ієрархічних рівнів доцільно попередньо закріпити реалізацію дозвільних функцій з виконання платежу. В момент початку

безготівкового переказу відповідному керівнику видаватиметься повідомлення про параметри платежу та дозвіл чи заборону трансакції. В обліковій політиці підприємства доцільно вказати грошовий поріг, досягнення якого передбачає запит санкції облікового та управлінського працівника. Якщо ліміт не перевищено, то запит не відбувається. І навпаки, у випадку здійснення безготівкової трансакції на понадлімітний обсяг потрібний почерговий дозвіл декількох фахівців з обліку та управління. Таким чином реалізується кіберзахист грошових трансакцій та забезпечується персоналізація відповідальності за грошові операції.

Застосування гібридної системи усуває процедуру складання паперового первинного документа. Не завжди можливо сформувати первинний розрахунковий документ у традиційній типовій формі. Враховуючи конфіденційність криптовалют, складно ідентифікувати особу платника, що не дає змоги заповнити основний реквізит будь-якого первинного документу. В автоматизованій системі обліку зазначається лише код грошової трансакції, що засвідчує погашення пов’язаної заборгованості. Роль традиційної банківської виписки, на основі якої формувалися облікові проведення, на нашу думку, в обліку за умови електронних переказів суттєво зменшується. Уся первинна інформація про рух електронних грошей та криптовалют за певний період надходить до бухгалтера, який в оперативному режимі має змогу моніторити залишки коштів на рахунках.

На основі електронної первинної інформації про зарахування коштів на рахунок підприємства, яка в автоматичному режимі оперативно надходить у бухгалтерію, автоматизовано можуть здійснюватися подальші облікові процедури. Передбачається, що коли покупець чи замовник продукції зі персонального електронного гаманця дає дозвіл на перерахування електронних грошей чи криптовалют, відбувається автоматичне внесення у систему обліку господарських операцій та формування облікових проведень. Аналогічно, і в одержувача надходження через гібридну систему інформації про зарахування безготівкових коштів на електронний гаманець ініціює автоматичне формування відповідного запису на рахунках бухгалтерського обліку в

програмному забезпечені. Схема інформаційних потоків в умовах автоматизованого управлінського обліку і контролю грошових засобів на основі застосування гібридної системи платіжних операцій електронними грошима, криптовалютами, коштами на рахунках в банку з інтеграцією функцій технологій блокчейн, «Інтернет-банк» та «Клієнт-банк» подано на рис. 2.4.

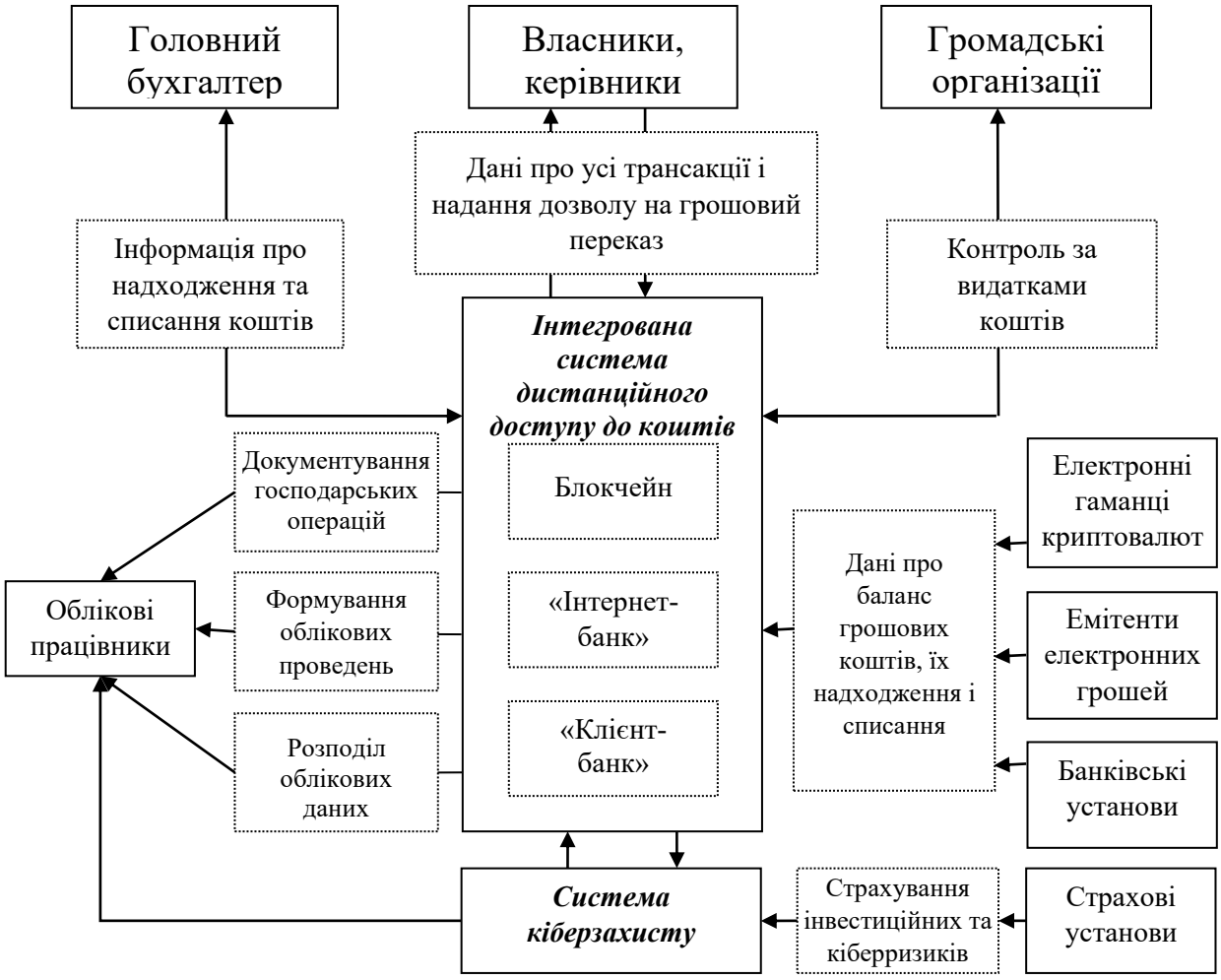


Рис. 2.4. Система обліку і кібербезпеки безготівкових переказів з використанням криптовалют та інших електронних грошей

Джерело: сформовано автором

Феномен криптовалют та інших електронних грошей формує значний потенціал для автоматизації обліку на підприємстві. Можливість вбудованої підтримки персональних гаманців електронних грошей в мобільних пристроях забезпечує безготівковий розрахунок за придбані

товари (послуги) аналогічно банківським карткам. Криптовалюта поступово набуває практичного застосування і перетворюється на ефективний засіб грошового обігу, що вимагає її визнання з позиції теорії економіки та обліку як еквівалента грошових коштів.

З використанням гібридної системи зменшується потреба у використання готівки як платіжного засобу та, відповідно, каси як організаційного підрозділу в організаційній структурі підприємства. За необхідності готівкові кошти можуть бути отримані у банкоматах. Значно зменшується кількість працівників підприємства, які оперують грошовими коштами та мають доступ до облікової інформації, що позитивно впливає на кібербезпеку підприємства. Усі інформаційні процеси виконуються без прямої участі облікових фахівців, що мінімізує вплив людського чинника на кібербезпеку підприємства.

В гібридній системі доцільно зберігати дані електронних гаманців для отримання доступу до залишку криптовалют. За даними статистики біля 25% власників криптовалюти втратили ключі доступу [137]. Використання гібридної системи попереджає втрату ключів доступу до електронного гаманця і, відповідно – усіх криптоактивів.

Аналогічно, доцільно передбачити функцію контролю випадкових транзакцій користувачами. Для цього необхідно встановити часовий лаг між списанням грошових коштів з рахунку відправника та зарахуванням одержувачу. За цей період часу обліковий чи управлінський персонал може перевірити коректність платіжних реквізитів і, у випадку виявлення помилки, скасувати остаточне виконання електронної трансакції.

У гібридній системі також доцільно передбачити страхування криптоактивів від інвестиційних та кіберризиків. При передачі криптобіржі електронних коштів їхній власник фактично не володіє активами, а отримує до них доступ при вході в інформаційну систему. У випадку кібератаки на інформаційну систему біржі можлива втрата кібервалюти. Якщо біржа оголошує себе банкрутом, повернення кіберактивів уже неможливе. Аналогічно й значні негативні стрибки у вартості кібервалюти можуть призвести до значних збитків у їхніх власників. Корисним й ефективним є страхування різних видів ризиків у

процесі зберігання та оперування криптовалютами. У гібридній системі доцільно розміщувати пропозиції різних страхувальників щодо страхування криптоактивів. Власник криптовалюти на конкурентних основах може обирати оптимальний страхувальний пакет послуг.

2.3. Використання технології Інтернету речей в автоматизації обліку та кіберзахисті

Цифровізація соціально-економічних процесів ґрунтується на повселюдному використанні мережі Інтернет. Надання доступу стейкхолдерам до глобальної комунікаційної мережі є запорукою оперативності, достовірності, своєчасності та зручності обробки облікової інформації. Електронні комунікації забезпечують об'єднання учасників інформаційного процесу в спільноту задля спільного виконання функціональних обов'язків. Мережа Інтернет є інформаційним інтегратором джерел інформаційних ресурсів, баз їхнього сховища, електронних сервісів й технологій обміну інформацією. Інформаційною основою кругообігу соціально-економічної інформації є система обліку, яка є інформаційним генератором та комунікатором.

Зростання рівня побутового проникнення Інтернет-технологій призвело до виникнення нового фундаментального явища – Інтернету речей. Технологія Інтернету речей (Internet of Things, IoT) – сукупність знань про використання програмно-технічного комплексу, який містить технологічні датчики, виконавчі механізми, сенсорні монітори та мікрокомп'ютери у формі елементів одягу, побутової техніки, транспортних засобів, виробничого обладнання тощо, які з'єднані з мережею Інтернет для взаємодії з навколишнім світом чи комунікацій між собою та людиною.

Проникнення IoT-технології у господарські процеси суб'єктів господарювання спричинило фундаментальні зміни першочергово в автоматизованій обробці облікової інформації. Проте разом з

позитивними функціональними можливостями використання IoT-пристроїв існують значні перешкоди імплементації технології Інтернету речей. Надання масового відкритого Інтернет-доступу до побутових та господарських пристроїв створює загрози функціонуванню підприємств. Кіберзагрози пов'язані з можливістю витоку конфіденційної облікової інформації, інформаційного шпіонажу, кібератак, кібертероризму, що визначає актуальність організації ефективної системи кіберзахисту в умовах застосування IoT-технологій.

Ринок систем кіберзахисту IoT-технологій щороку зростає і за прогнозами до 2025 року досягне 30,9 млрд дол. США (рис. 2.5). Перманентний щорічний приріст показника, починаючи з 2016 року, становить 15 %, що свідчить про перспективність досліджень у сфері кіберзахисту інформації в умовах застосування IoT-пристроїв.

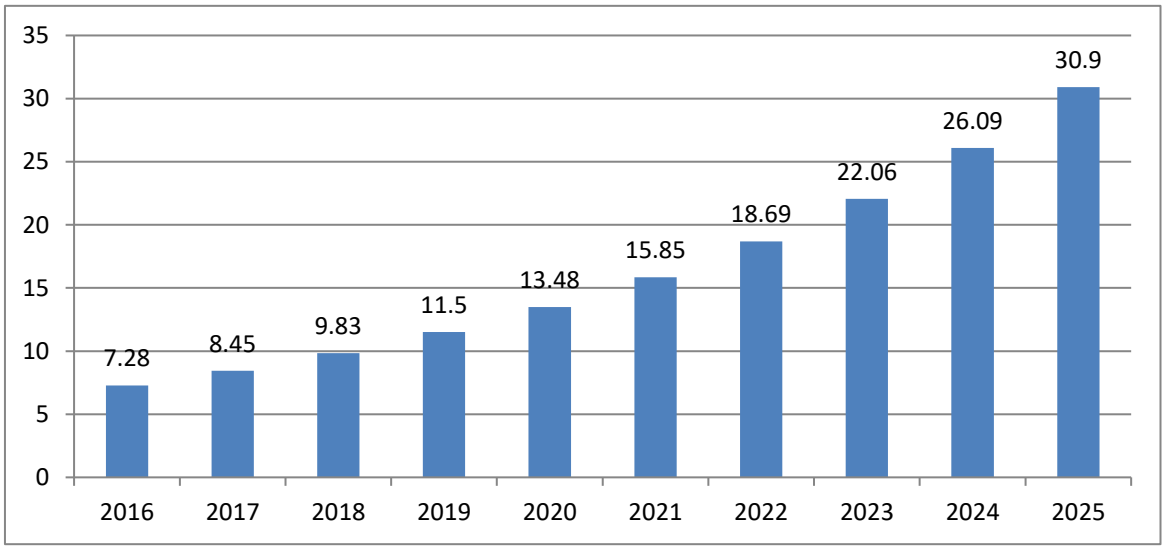


Рис. 2.5. Розмір глобального ринку IoT кібербезпеки у 2016-2025 рр. (в мільярдах доларів США)

Джерело: сформовано на основі [168]

В науковому просторі присутні численні праці, присвячені забезпеченню кіберзахисту підприємств з використанням технології IoT. Більшість з них ґрунтуються на імплементації блоково-ланцюговоого структурування даних (технології блокчейн в обробці інформації). Водночас науковці проводять оригінальні наукові дослідження щодо

перспективних варіантів кіберзахисту підприємств в умовах застосування IoT-пристроїв для господарських цілей.

Зокрема Kumar Gautam, Singh Om Prakash й Saini, Hemraj Šikanjić обґрунтували вплив Індустрії 4.0 на кібербезпеку підприємств, що потребує застосування новітніх комунікаційних технологій, серед яких важливе місце займає IoT [109]. Також Šikanjić Nedeljko, Avramović Zoran та Marinković Dražen запропонували структуру IoT інфраструктури, використання якої мінімізує кіберризики та кіберзагрози функціонування підприємства [164]. Аналогічно й Henry Matey Akwetey та інші дослідили перспективи використання технології IoT для кіберзахисту об'єктів критичної інфраструктури держав [93]. Aisenberg Michael й інші визначили напрямки державної та місцевої політики у сфері кібербезпеки через поєднання технологій IoT, хмарної обробки інформації та блоково-ланцюгового структурування даних [47]. Аналогічно й Smith Kane, Dhillon Gurpreet та Carter Lemuria розробили напрямки держаної політки у сфері кіберзахисту IoT-технологій на основі позиціонування «користувацьких цінностей» (інформаційних потреб користувачів) [170].

Rohan Rohani, Funilkul Suree, Pal Debajyoti та Thapliyal Himanshu пояснили вплив технології IoT в споживчому використанні на мінімізацію чинника людського ресурсу [152]. Роль штучного інтелекту в кіберзахисті IoT-технології також дослідили Kuzlu Murat, Fair Corinne та Güler Özgür [111]. Продовжили дослідження Chesney Steve, Roy Kaushik і Khorsandroo Sajad, які запропонували алгоритми машинного навчання для превентивного попередження активних кіберзагроз у сфері IoT [63].

У той же час Djenna Amir, Saidouni Djamel Eddine та Wafia Abada запропонувати прагматичні стратегії кіберзахисту підприємств від прояву кібератак з використанням IoT [73]. Іншу стратегію організації кібербезпеки у сфері IoT, що орієнтується на перманентній змін безпекових налаштувань, запропонували Mercado-Velazquez Andres, Escamilla-Ambrosio P. Jorge і Ortiz-Rodriguez Floriberto [123].

Проте науковці розкривають теоретичні та практичні аспекти забезпечення кіберзахисту в умовах застосування технології IoT з позиції обробки економічної інформації. Поза увагою в наукових дослідженнях

залишається облікова природа більшості інформації про соціально-економічні процеси на підприємстві. І лише поодинокі напрацювання одночасно стосуються бухгалтерського обліку та кіберзахисту. Наприклад, можна виділити наступні переваги та проблеми для ланцюжка формування бізнес-звітності підприємства із використання IoT:

– автоматизація збору інформації, необхідної для ведення діловодства та прийняття рішень з потенційною перевагою полегшення збору збільшеного обсягу інформації (більш детально та частіше) зі зменшенням помилок ручної праці;

– скорочення проміжку часу між подією та її записом для більш своєчасного прийняття рішення;

– сприяння оцінці діяльності та керованості бізнес-процесів;

– збільшення обсягів бухгалтерських даних, кількості дій та спостережень, зменшення безпосереднього прямого людського впливу.

Дослідник Smith E., що займається сучасними проблемами комп'ютеризації бухгалтерського обліку, визначає наступні переваги об'єднання бухгалтерського обліку з IoT: 1) Здатність відстежувати активи; покращене використання активів; 2) Економія витрат; 3) Покращення якості та моніторингу; 4) Кількісно визначені працівники – охорона праці; 5) Більш ефективний аналіз доходу; 6) Поліпшення прогнозування; 7) Покращене управління ризиками; 8) Краще прийняття рішень та ефективність бізнесу [169].

Важливою здатністю IoT-технології є збір інформації про події та явища, що є цінним інформаційним ресурсом для обліку та управління підприємством.

Як доводять Легенчук С.Ф., Ородиський М.П. та Майстренко Н.М., необхідно врахувати, що IoT стосується процесів обробки даних з різних об'єктів, які є вхідними даними з позиції бухгалтерських інформаційних систем, то можна констатувати існування впливу IoT на методи збору та обробки бухгалтерських даних, а також їх контроль. Використання датчиків для одержання первинної інформації про речі та людей (працівників бухгалтерської служби) та забезпечення їх взаємозв'язку в

мережі сприятиме підвищенню ефективності функціонування облікових інформаційних систем на підприємствах [114, с.12].

Отримання облікових даних з використанням IoT-технології може відбуватися у значній територіальній віддаленості відправника від одержувача інформації. Місце здійснення господарської інформації, обладнане технологічними датчиками, можливо розміщувати на значних просторових відстанях від обліково-управлінського підрозділу. Оскільки первинні облікові дані збираються та реєструються автоматично, то відсутня необхідність надсилання облікових чи управлінських працівників у місце виникнення фактів господарської діяльності.

Використання технології Інтернету речей мінімізує участь облікових фахівців у процесі збору первинних даних. Ідентифікація, збір, реєстрація та первинна обробка інформації відбувається зі застосуванням технологічних датчиків, що є складовими Інтернету речей. Оскільки більшість інформаційних процесів відбувається повністю автоматизовано, зменшується потреба у залученні людських ресурсів в організацію обліку. З людським чинником пов'язані невизначеність, ймовірність помилок, фінансових махінацій, неточностей, недотримання встановлених термінів тощо. Як наслідок, збір облікових даних з використанням обладнання, під'єднаного до мережі Інтернет, відбувається з високим рівнем кіберзахисту. Зменшення впливу людського чинника на інформаційні процеси є запорукою ефективної організації контролю функціонування підприємств.

Використання IoT-технології трансформує процес надання аудиторських послуг. Аудиторські компанії отримують впевненість в достовірності облікових даних, отриманих з використанням сучасних комп'ютерно-комунікаційних технологій. Аудитори можуть пропускати етап документальної перевірки фінансово-господарської діяльності підприємства, оскільки більшість облікових даних збираються в електронній формі. Аналогічно й проведення інвентаризації та інших видів матеріальних перевірок значно спрощується з використанням технологічних датчиків. Інформація про фактичну наявність активів чи пасивів підприємства автоматично порівнюється з обліковими записами в

перманентному режимі. У момент виявлення відхилень здійснюється інформування облікових та аудиторських працівників з формуванням інвентаризаційних описів. Виконання більшості аудиторських процедур може відбуватися віддалено від об'єкта аудиторського контролю. Дистанціювання в реалізації аудиторських послуг є корисним в умовах пандемічних очікувань суспільства.

Також облікові та аудиторські фахівці через використання IoT-технології отримують облікову інформації в режимі реального часу. Завдяки глобальним електронним комунікаціям значно мінімізується часовий лаг між виникненням облікових даних та їхньою передачею до облікового підрозділу. Як наслідок, автоматично зібрана облікова інформація завжди є своєчасною та актуальною.

Унаслідок необхідності перманентного під'єднання технологічних датчиків до мережі Інтернет, виникають значні кіберзагрози функціонуванню підприємству (табл. 2.1).

Таблиця 2.1

Глобальні загрози та проблеми безпеки в Інтернеті речей (IoT)

№	Загрози та проблеми безпеки в Інтернеті речей (IoT)	%
1	Атаки на пристрої IoT, які можуть вплинути на критичні операції	33
2	Відсутність персоналу для впровадження безпеки IoT	32
3	Захист конфіденційних даних, створених пристроєм IoT (шифрування, токенізація тощо)	31
4	Ідентифікація або виявлення конфіденційних даних, створених пристроєм IoT	27
5	Втрата або крадіжка пристроїв IoT	27
6	Відсутність систем безпеки та засобів контролю в середовищі IoT	26
7	Порушення конфіденційності, пов'язані з даними, створеними пристроєм IoT	26
8	Відсутність ефективного контролю доступу/автентифікації пристрою	26
9	Відсутність галузевих стандартів для захисту пристроїв IoT	25
10	Перевірка цілісності даних, зібраних пристроями IoT (ідентифікація пристрою, надання)	7
11	Привілейований доступ користувачів до пристроїв IoT	2

Джерело: систематизовано на основі [97]

Перш за все кібератаки орієнтуються на обмеження або припинення доступу до мережі Інтернет для завдання критичної шкоди діяльності підприємств (33 % від глобального показника кількості кібератак). Втрата Інтернет доступу може призвести не лише до блокування передачі зібраних облікових даних, але й до повного призупинення діяльності суб'єктів господарювання. Керівництву суб'єкта господарювання слід забезпечити резервні джерела під'єднання до глобальної комунікаційної мережі. Корисним є дуплексний доступ до мережі Інтернет через кабельних провайдерів та операторів стільникового зв'язку, що сприяє попередженню неочікуваного відімкнення Інтернет-доступу.

Оскільки IoT-датчики та пристрої з'єднані з глобальною мережею, існує імовірність викрадення облікових даних з наступною їхньою передачею стороннім особам. Пристрої IoT-технології можуть використовуватися зловмисниками для персонального та промислового шпіонажу. Наприклад, елементи одягу з функціями Інтернет-комунікацій здатні збирати інформацію про місце перебування, біологічні параметри життєдіяльності та особисті електронні комунікації персоналу підприємства.

Проте ці ж дані можуть бути корисні для управління діяльністю облікових фахівців у процесі виконання ними функціональних обов'язків. Доцільно моніторити час виконання персоналом певних функціональних робіт чи процедур. На основі операграми робочого дня фахівців можливо визначати способи оптимізації функціонування працівників. З використанням інформації з особистих IoT-пристроїв про затрачений робочий час можливо визначати розмір заробітної плати штатних та найнятих працівників підприємства. Вартість послуг сторонніх (аутсорсингових) облікових чи аудиторських інституцій також залежить від кількості людино-годин роботи.

Інформація про роботу працівників з IoT-пристроїв, яка потрапила до сторонніх осіб, може використовуватися для з'ясування механізму ціноутворення професійних послуг обліковими та аудиторськими фірмами, що є елементом неконкурентної боротьби. Натомість технологічні датчики технології IoT, що вмонтовані у виробниче

обладнання, можуть надсилати облікову інформацію також і зловмисникам. Причиною високого рівня кіберзагроз у сфері перехоплення облікових даних третіми особами є недостатня увага використанню надійних паролів доступу до IoT-пристроїв. Керівництво підприємства упускає у безпековій політиці моменти зміни стандартних логінів і паролів при використанні технологічних датчиків та пристроїв. Рекомендованим є розробка специфічних регламентів використання криптографічних систем захисту, частої зміни засобів ідентифікації осіб для доступу до IoT-пристроїв. Акцентування уваги на кібербезпеці доцільно здійснювати у двох напрямках: особистому захисту індивідуальних пристроїв IoT-технології працівників підприємства та глобальному захисту облікової інформації, отриманої з технологічних датчиків виробничого обладнання.

Зловмисники після отримання доступу до пристроїв технології-IoT можуть змінювати параметри їхньої роботи. В такому випадку треті особи отримують повне управління господарськими процесами, що обслуговуються технологічним обладнанням. Можливі перебої у реалізації господарських циклів, навмисне погіршення якості продукції, надмірне витрачання виробничих ресурсів, виведення з ладу обладнання, що, в кінцевому результаті, призведе до зростання витрат підприємства та економічного банкрутства.

Більш загрозливим для кібербезпеки підприємств є підвищення прав доступу для актуальних працівників підприємства або наділення такими правами сторонніх осіб з метою несанкціонованого потрапляння на територію підприємства. Пошкоджені зловмисниками IoT-пристрої, які є технологічною частино безпекової системи підприємства, можуть здійснювати аутентифікації сторонніх осіб із наданням права доступу до конфіденційної інформації. Треті особи при проникненні в підрозділи підприємства потенційно здатні до здійснення шпіонажних, саботажних, терористичних та деструктивних дій.

Для превентивного уникнення несприятливих для кібербезпеки подій необхідною є багатоступенева ідентифікація осіб, які запитують право на інтервенцію в інформаційний або територіальний простір підприємства.

Доцільно паралельно здійснювати автоматичну аутентифікація осіб з використанням IoT-пристроїв та підтвердженням працівниками безпекового підрозділу права на доступ до особливо важливої та конфіденційної інформації підприємства. В пунктах фізичного перетину території суб'єкта господарювання рекомендовано розміщувати місця візуального контролю безпековими працівниками коректності роботи системи автоматичного пропуску. Додаткове залучення людського ресурсу до кіберзахисту підприємства мінімізує ризики стороннього впливу на пристрої IoT, на використанні яких ґрунтується технологічна компонента кібербезпеки підприємства.

Для забезпечення кіберзахисту облікової інформації також важливим є моніторинг комунікаційних каналів та маршрутів. Доцільно контролювати відповідність інформаційних потоків попередньо встановленій схемі кругообігу облікової інформації. Якщо виявлено факти розбіжностей, то виникають підозри про витік конфіденційної інформації. Передача інформації з місця її збору до бази даних має відбуватися за регламентованими комунікаційними каналами. Використання ненадійних електронних комунікацій ставить під сумнів достовірність облікової інформації, що може бути причиною втрати її споживчої цінності.

Перманентне надходження великих інформаційних потоків з IoT-пристроїв створює значне інформаційне навантаження на програмно-технічні ресурси підприємства. З метою врахування необхідності обробки значних інформаційних масивів доцільно впроваджувати у діяльністю новітню комп'ютерно-комунікаційну форму обліку. Така форма обліку здатна врахувати зростаючу мережу електронних комунікацій підприємства, що усуває прояв таких комунікаційних бар'єрів, як: дублювання, суперечність різних інформаційних джерел, конкуренцію, погане сприйняття, незрозумілість, неналежну порівнюваність облікової інформації тощо.

Також зловмисники можуть використовувати пристрої IoT-технології для DoS/DDoS атак, які призводять до відмови штатного функціонування програмно-технічного забезпечення. IoT-пристрої можуть генерувати безладні запити до автоматизованої системи обліку, що може призвести до

блокування обробки облікової інформації. Для забезпечення кібербезпеки підприємства необхідним є застосування методів попередження та усунення наслідків DoS/DDoS кібератак не тільки на комп'ютерне обладнання підприємства, але й на всі пристрої, що є складовими IoT-технології. Додатковим заходом для організації кіберзахисту облікових ресурсів є їхнє відокремлення від інших видів інформації, які не мають економічної цінності для керівництва підприємства. Основні напрямки використання IoT-технології для подолання кіберзагроз в обліковій та безпековій сферах відображені на рис. 2.6.

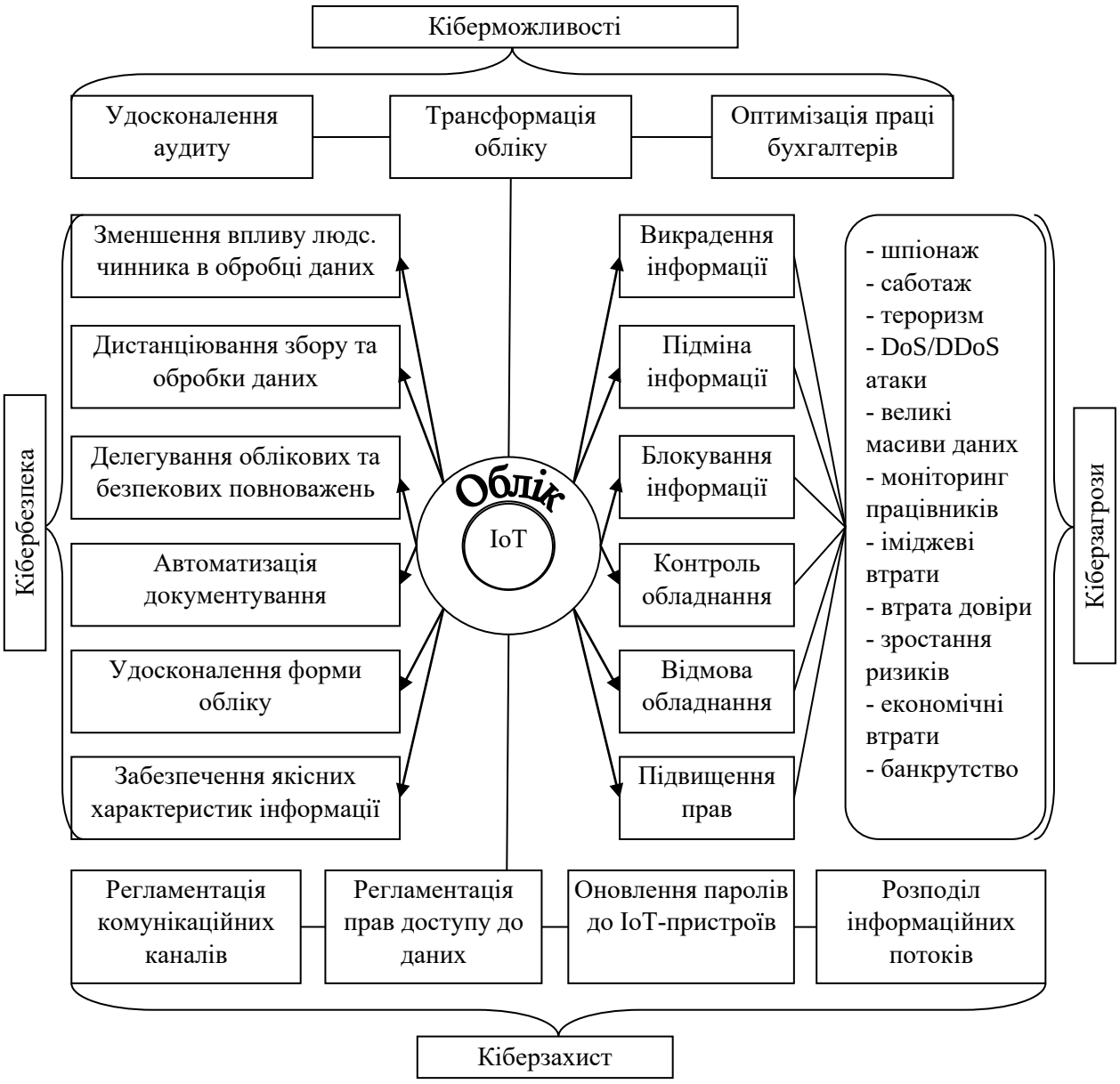


Рис. 2.6. Використання технології IoT для цілей обліку та кіберзахисту

Джерело: сформовано автором

Використання технології Інтернету речей в бухгалтерському обліку створює можливості для подолання загроз функціонуванню підприємств у частині забезпечення його кіберзахисту. Реалізація потенційних переваг застосування IoT-пристроїв створює сприятливі умови для забезпечення кібербезпеки підприємств. Натомість, ризики імплементації технології IoT значно мінімізуються за умови ефективної організації бухгалтерського обліку на підприємстві як базису налагодження кіберзахисту інформаційних потоків.

2.4. Облік оплати праці з використанням технології біометрії для забезпечення кіберзахисту підприємств

У діяльності суб'єктів господарювання досить часто використовується прохідна система пропуску працівників на територію. Організація пропускного режиму на підприємстві передбачає контроль за присутністю персоналу на робочому місці та унеможливлення крадіжок чи інших махінацій з матеріальними цінностям. В умовах комп'ютеризації обліку і управління господарською діяльністю використовується автоматизована система контролю, яка призначена для надання дозволу на прохід персоналу, проїзд транспортних засобів або переміщення матеріалів через вхід (вихід) контрольно-пропускних пунктів зон обмеження доступу [1]. Технічними елементами автоматизованої системи пропуску є: турнікети звичайні і настінні; турнікети для проходу в коридорах; шлюзові кабіни; автоматичні двері; роторні турнікети; обертові двері; дорожні блоки; шлагбауми; паркувальні системи; круглі розсувні двері; повнозростові турнікети; розсувні турнікети, камери відеоспостереження тощо [1], які встановлюється у місцях перетину території підприємства або функціональних приміщень. Функціонує система на принципі персоніфікованої ідентифікації персоналу в момент перетину інформаційно-просторових меж підприємства. Унікальним

ідентифікатором у більшості випадків є індивідуальна чіпована картка з особистими даними працівника.

Реєстрація автоматизованою системою факту прибуття та вибуття працівника з підприємства є підставою для визначення відпрацьованого ним часу. На практиці, як зазначає Янчев А.В., використовуються різні варіанти автоматизованого збирання та обробки інформації щодо обліку праці і заробітної плати, вибір яких в значній мірі залежить, з одного боку, від типу виробництва, особливостей його організації і технології; організації і форми оплати праці; застосованих форм первинних документів і їх структури; системи централізованого, децентралізованого або змішаного облікового процесу, форм обліку тощо; з другого боку – типу, класу, комплектності застосованих обчислювальних машин і засобів периферійної техніки; методів організації інформаційного забезпечення; ступеню механізації і автоматизації нормативно-планових розрахунків тощо [44, с. 217].

Проте дієвість такого обліку залишається сумнівною у випадку наявності працівника на підприємстві, але не виконання ним функціональних обов'язків. Працівник може перебувати в приміщеннях, які безпосередньо не відносяться до сфери його компетентності. Іншими словами, наявність особи на підприємстві ще не гарантує виконанням нею професійних функцій, що не може вважатися ефективним способом обліку відпрацьованого часу та заробітної плати. Також чужою індивідуальною карткою може скористатися інша особа, що порушує принцип персоніфікованої ідентифікації працівника. Для уникнення організаційно-функціональних обмежень автоматизованої ідентифікації персоналу для цілей обліку робочого часу та заробітної плати доцільно використовувати сучасні технології біометрії. Біометрія – сукупність автоматизованих методів і засобів ідентифікації людини, заснованих на її фізіологічній або поведінковій характеристиці [3].

Технологія біометричної ідентифікації набуває значної популярності у комерційному використанні. Відповідно до досліджень Global Biometrics in Workforce Management Market у 2019 році серед компаній Північної Америки та Європи, які використовують сучасні комп'ютерно-

комунікаційні технології, 62 % опитуваних застосовують можливості біометричної ідентифікації осіб (у 2021 році – 86 %). Більшість суб'єктів господарювання (51 %) реалізують біометрію за допомогою мобільних телефонів. Проте, все активніше використовуються системи часового контролю робочих місць (20%), розумних замків доступу до приміщень (18 % – доступ до серверного обладнання і 14% – доступ до офісних приміщень), переносні девайси як елементи одягу (5 %) та інші (рис. 2.7) (за даними Global Biometrics in Workforce Management Market [83]).

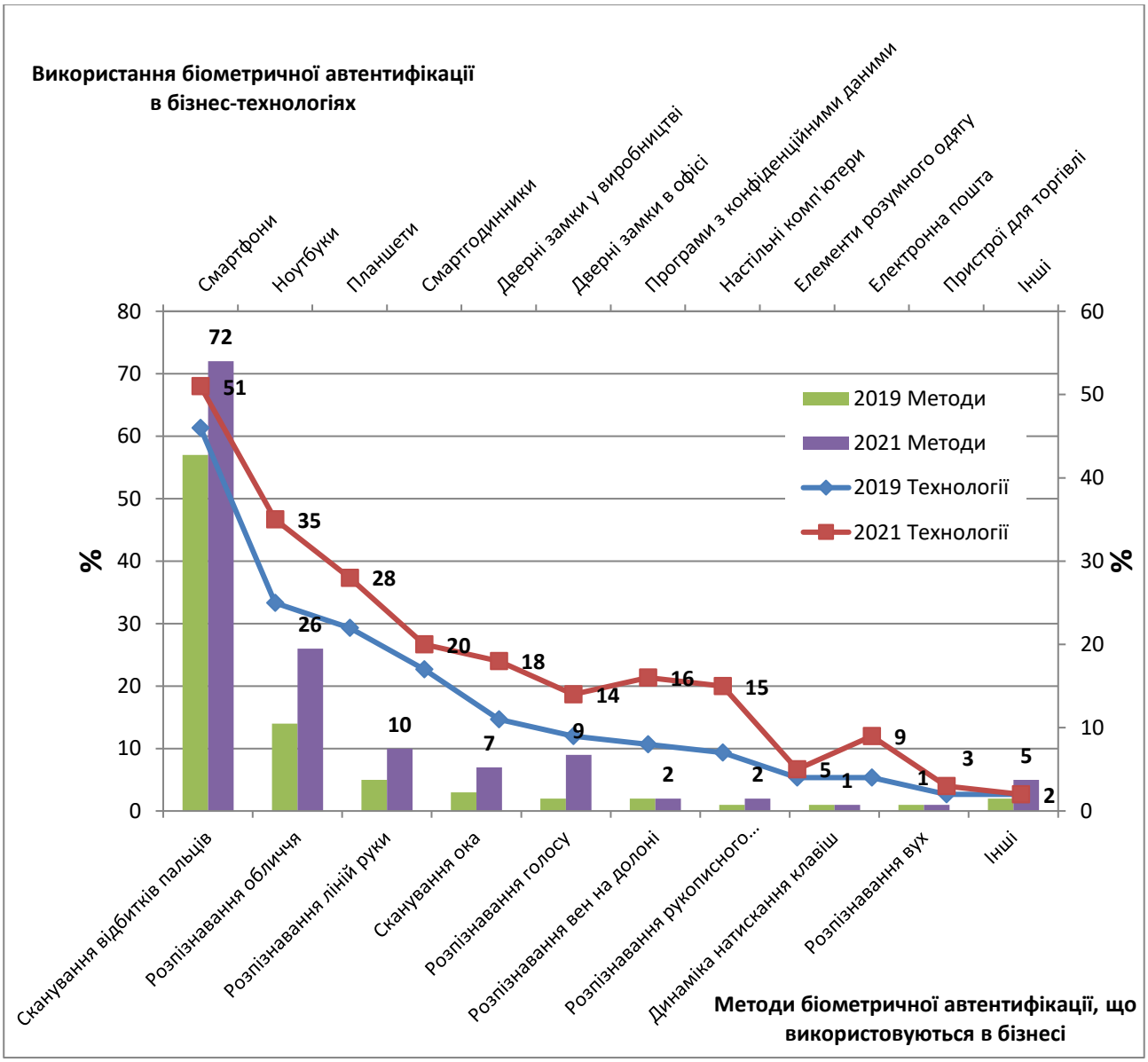


Рис. 2.7. Технології та методи біометричної аутентифікації в бізнесі

Джерело: сформовано на основі [83]

Решта суб'єктів господарювання, плануючи впровадження технологій біометричної ідентифікації працівників, зважають на організаційно-функціональні бар'єри та ризики (табл. 2.2). На думку опитуваних IT експертів, за даними дослідження Global Biometrics in Workforce Management Market, до найбільш значущих бар'єрів відносяться: значна вартість технології (67 %), надійність функціонування (59 %); до ризиків – можливість хибного спрацьовування (64 %), махінації з підставними зразками біометричних даних (57 %). Наведені обмеження у реалізації можливостей біометрії вирішуються з подальшими науково-технічним розвитком технологій. Проте, подолання наступного бар'єру (необхідність управління біометричними даними – 47 %) та ризику (відсутність стандартів і методик використання даних – 50 %) потребує досліджень у сфері практичного використання технологій біометричної ідентифікації, зокрема для цілей бізнесу.

Таблиця 2.2

Перешкоди впровадження біометричної автентифікації на робочому місці

Перешкоди для впровадження біометричної автентифікації на робочому місці	**% опитаних**	**Занепокоєння щодо безпеки використання біометричної автентифікації на робочому місці**	**% опитаних**
Вартість технології	67	Ризики помилкових спрацьовувань	64
Недостатня надійність	59	Ідентифікатори можуть бути скопійовані	57
Складність управління біометричними даними	47	Відсутність стандартів і методів використання	50
Вимоги до оновлення системи	42	Ризики викрадення біометричних даних	48
Супротив співробітників	42	Ризики відповідності стандартам	37
Складність впровадження	40	Ідентифікатори не можна відкликати	35
Вимоги до перенавчання персоналу	38	Інше	6

Джерело: систематизовано на основі [83]

При дослідженні можливостей господарського використання технології біометричної ідентифікації науковці визначили перспективність розробок у сфері збору даних про час роботи та місце перебування персоналу підприємства. Наприклад, Fubara-Manuel I.

дослідила методику використання технологій біометричної ідентифікації для контролю за переміщенням персоналу підприємств, за входом (виходом) за периметр різних приміщень чи територій [80]. Безпекові аспекти ідентифікації фактів просторового переміщення персоналу із впливом на доступ до інформаційно-матеріальних ресурсів дослідили Li B., Ponson G., Ezzahi Y., що визначає важливість технології біометрії у забезпеченні кібербезпеки підприємства [115]. В продовження досліджень кіберзахисту Sinno S. і Hawley C. науково пояснили засоби контролю доступу до інформації на основі біометричної ідентифікації у частині моніторингу роботи працівників підприємства [165]. Аналогічно Sun Zhenjun, Li Qi, Liu Yunfan та Zhu Yuhao серед перспективних можливостей біометрії виокремлюють можливість ідентифікації особи для контролю за переміщенням не тільки по території підприємств, але й часу виконання функціональних обов'язків [177]. Продовжив дослідження Boonkrong S., який визначив особливості оплати праці на основі контролю доступу працівників до комп'ютеризованого обладнання за логінами і паролями [61].

Технології біометричної ідентифікації активно використовуються у програмно-технічному забезпеченні систем контролю робочого часу та дотримання трудової дисципліни. До основних функцій таких систем відносять:

– формування графіків роботи підприємства (організації) в цілому, його структурних підрозділів і співробітників;

– підрахунок кількості відпрацьованого часу співробітниками згідно з графіками їх роботи;

– контроль відхилень від робочих графіків (нештатних ситуацій);

– контроль доступу працівників на територію підприємства тощо [38].

Але у системах контролю робочого часу та в наукових працях дослідників з біометричної ідентифікації осіб поза увагою залишається можливість автоматизації обліку й контролю робочого часу та заробітної плати працівників суб'єктів господарювання. У той же час науковці виокремлюють нові тренди в автоматизації обліку виплат працівникам, що

обумовлюються розвитком комунікаційних технологій та пандемічним дистанціюванням у процесі виконання працівниками функціональних обов'язків. Зокрема, Очеретько Л. М., Удовиченко Г. І. розглядають трансформацію робочого процесу працівників та особливості обліку заробітної плати в умовах глобальної пандемії COVID-19 [140]. Neil G. визначив основні тренди в оплаті праці у негрошовій формі, що передбачає перехід на дистанційну роботу та отримання винагороди у електронних валютах разом із автоматизацією обліку заробітної плати [135]. Основним трендом у забезпеченні робочого процесу є імплементація інформаційно-комунікаційних технологій для забезпечення дистанційного або ізольованого виконання функціональних обов'язків. На необхідності обмеження доступу до приміщень підприємства для забезпечення біозахисту працівників також наголошують Fletcher J., Gillum D., Moritz R. та Schwartz A., що вносить зміни в облік та управління робочим процесом [79].

Науковець Gupta W. розробив унікальну модель визначення розміру зарплати найнятого працівника на основі оцінки професійно-особистісних характеристик претендентів за списком вакансій на сайтах працевлаштування [89]. Аналогічно й Kuo Jong-Yih, Liu Chien-Hung та Lin Hui-Chi на основі технології «глибокого навчання» запропонували методику автоматизованого визначення та обліку заробітної плати на основі ряду змінних показників за довільні періоди часу [110]. Спільною науковою позицією для усіх науковців, як стверджують Ревенок В.І. та Мамчур О.С., є формування основних вимог до системи обліку робочого часу та заробітної плати персоналу в умовах використання комп'ютерно-комунікаційних технологій:

– інтеграція кадрового обліку, обліку праці та її оплати в єдине ціле;

– централізація обробки інформації з обліку праці та її оплати;

– автоматизований збір інформації про вихід працівників на роботу та відпрацьований ними час;

– автоматизація типових розрахункових операцій;

– автоматизований контроль за переміщенням працівників по території підприємства та доступом до інформації [34, с.22].

Технічною компонентою автоматизованої системи пропуску працівників є сканери біометричних параметрів, які встановлюються у місцях перетину просторових меж підприємства та виробничо-офісних приміщень. Виробниче обладнання та комп'ютеризовані робочі місця також обладнуються засобами біометричної ідентифікації працівників. За кожною одиницею основних засобів закріплюється перелік відповідальних осіб, яким надається доступ до інформації та виконання посадових обов'язків. Автоматизована система ідентифікації персоналу використовується у більшості випадків для безпекових функцій.

Інформацію про надання санкціонованого доступу до приміщень підприємства та обладнання пропонується також використовувати для обліку відпрацьованого часу персоналу. Біометрична ідентифікація працівників у процесі роботи машин та інструментів розцінюється як виконання посадових обов'язків. Час, проведений за обладнанням, може бути визнаний робочим часом працівника, що впливає на нарахування заробітної плати. Схожий принцип оцінки відпрацьованого часу уже застосовується в автоматизованих робочих місцях комп'ютерних спеціалістів, початок і завершення робочого дня яких визначається через персоніфіковану ідентифікацію.

Основним проблемним моментом в автоматизації обліку відпрацьованого часу є контроль за роботою працівників, які можуть знаходитися на робочому місці, але не виконувати функціональні обов'язки. Досить ефективним в такому випадку є використання відеоспостереження. Візуальна ідентифікація забезпечує контроль за переміщенням працівників між приміщеннями та часом перебування на підприємстві для забезпечення його кіберзахисту. Також автоматизована система пропуску на основі біометричної ідентифікації персоналу є корисною для розмежування людських потоків у приміщеннях підприємства з метою забезпечення біологічного захисту. Контроль надмірного просторового скупчення осіб та дотримання правил особистої гігієни у приміщеннях є важливою складовою попередження і уникнення біологічних загроз в умовах пандемії COVID-19.

Перелік постійних та змінних даних щодо переміщення персоналу по території підприємства та його приміщеннях з використанням технології біометрії для цілей обліку та кіберзахисту подано в інформаційній моделі на рис. 2.8. В основі автоматизованої системи обліку робочого часу доцільно використовувати єдину базу даних. Інтегрована база даних повинна містити усю інформацію про працівників підприємства: вік, стаж, кваліфікацію, освіту, посаду, посадові обов'язки, право доступу до інформації, методику розрахунку оплати праці, наявні пільги щодо оподаткування заробітної плати, особливі умови, що визначають право на доплати чи компенсації. Всі документи, які стосуються кадрової політики, вносяться в інформаційну систему.

Для забезпечення достовірності та своєчасності обліково-контрольних процедур на підприємствах, які використовують системи біометричної ідентифікації, рекомендовано обрати хвилину як базову одиницю виміру відпрацьованого часу. Хвилина робочого часу – оптимальна калькуляційна одиниця, що дозволяє організувати більш ефективний облік заробітної плати. Також з використанням похвилинного обліку можливо здійснювати деталізований контроль запізнень працівників, відлучення з робочих місць або несанкціонованого перетину меж підприємства в робочий час. В кінці звітного періоду на основі даних про сумарні непродуктивні втрати робочого часу рекомендовано автоматично коригувати розмір заробітної плати.

Інформацію про персональне відхилення робочого періоду від нормативних показників доцільно оперативно надсилати персоналу. В кожного працівника появляється можливість самоконтролю та коригування робочого часу. Мінімізується можливість маніпулювання обліковою інформацією працівником при самостійному заповненні листів відпрацьованого часу щодо закруглення до повної робочої години. У системі біометричної ідентифікації можливо автоматизовано фіксувати хвилину початку та завершення робочого часу посадової особи, що забезпечує справедливе визначення заробітної плати часу та мінімізує конфлікти між працівниками та працедавцями.

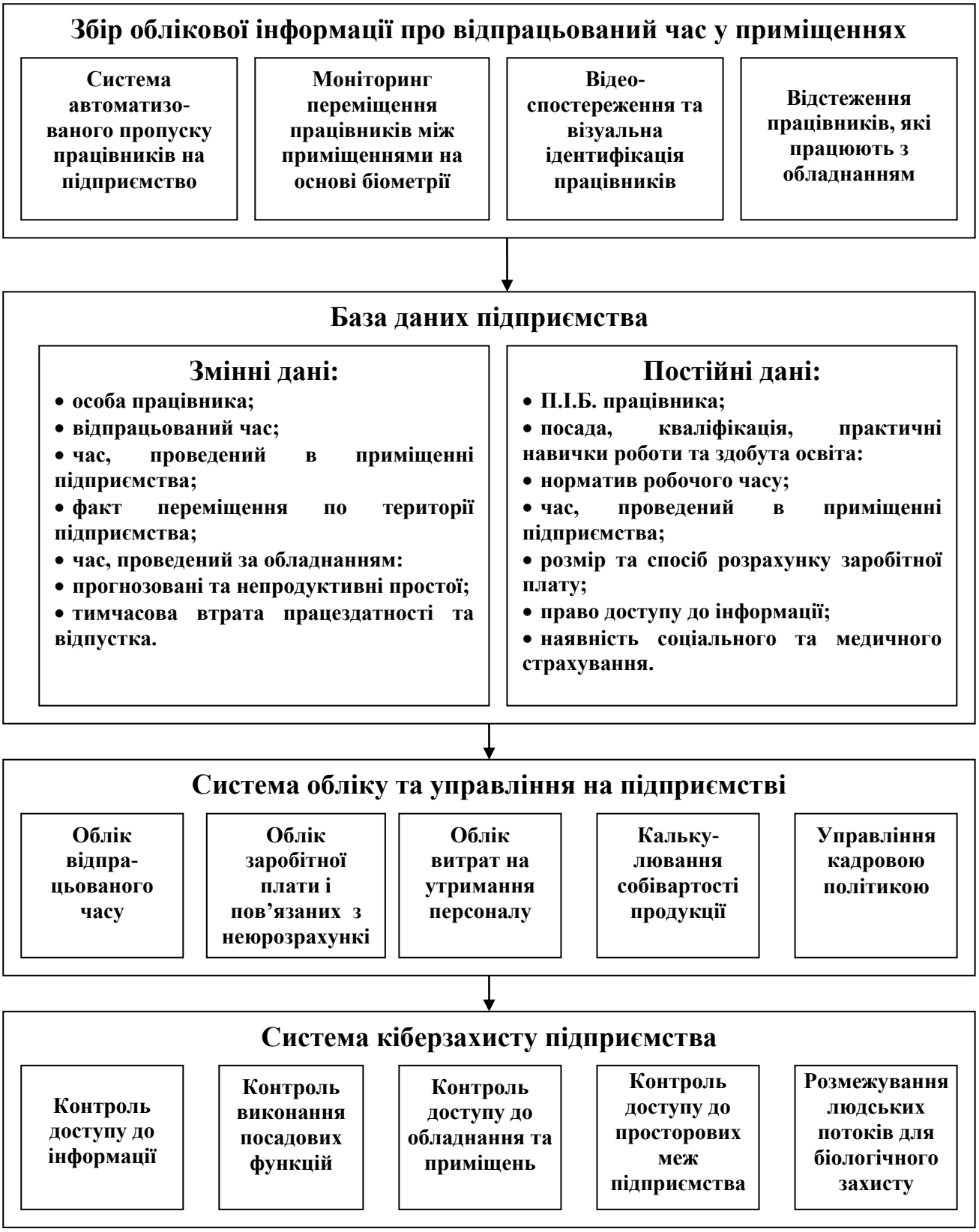


Рис. 2.8. Інформаційна модель автоматизованого обліку відпрацьованого часу, заробітної плати на основі системи біометричної ідентифікації для забезпечення кібербезпеки

Джерело: сформовано автором

Облік робочого часу в хвилинах може використовуватися для стимулювання продуктивності праці осіб з нормативним фондом робочого часу. Похвилинний облік відпрацьованого часу актуальний для працівників, заробітна плата яких залежить від комбінованого поєднання різних видів робіт в межах запланованого часового періоду. Зокрема, для працівників з ненормованим робочим графіком, що працюють в умовах пандемії COVID-19 з дому з погодинною оплатою праці, виникає можливість достовірного обліку і контролю робочого часу. Працівник самостійно здійснює контроль та визначає тривалість робочої зміни.

Також в умовах біометричної ідентифікації працівників можливо вести облік відпрацьованого часу при роботі з розривом змін, що актуальне для підприємств з трьохзмінним режимом функціонування. Працівники можуть відлучатися з території підприємства (в тому числі для виконання завдань з дому) чи залишати виробничі приміщення на певний час. Система ідентифікуватиме факт переміщення посадової особи з підрахунком загального періоду виконання безпосередніх функціональних обов'язків. Окремо необхідно вести облік простоїв працівника, що передбачені технологічним процесом або специфікою діяльності підприємства. В часовому регламенті автоматизованої системи обліку необхідно прописати виробничий процес з можливістю невиконання працівниками посадових інструкцій, що не варто розцінювати як втрату робочого часу. Наприклад, після виготовлення певного обсягу продукції потрібний час на охолодження обладнання, завантаження нової порції сировини тощо. Іншими словами, після завершення виробничого циклу працівник згідно з посадовими інструкціями може покинути місце праці або виробниче приміщення і використати час вимушеного простою для власних потреб.

Забезпечується автоматизований контроль за особистими непродуктивними втратами часу, відслідковування відхилень від нормативного показника часу, необхідного на виконання одного виробничого завдання, виготовлення працівником однієї одиниці готової продукції, надання відповідної послуги посадовою особою тощо. Кожний факт відхилення доцільно фіксувати в єдиній базі даних у різних

аналітичних розрізах. Акумульовані дані є підставою для виявлення фактів зменшення продуктивності праці кожного працівника, що може бути сигналом для перегляду умов праці чи професійної перепідготовки відповідного фахівця.

На основі інформації про відпрацьований час, проведений на території підприємства чи вдома, можна автоматизовано нараховувати заробітну плату персоналу. Для автоматизації обліку і контролю заробітної плати доцільною є попередня фіксація тарифу за відпрацьовану одинцю часу за кожним видом виробничого приміщення підприємства, а також дистанційним виконанням функціональних обов'язків . Таким чином, необхідно встановити базові тарифні ставки оплати праці працівників за кожну хвилину перебування у певному виді приміщення (дому), для чого рекомендовано територію підприємства поділити на декілька зон. Також для забезпечення кібернетичної та біологічної безпеки необхідно обмежити право доступу персоналу до певних видів приміщень чи території підприємства.

Нарахування заробітної плати доцільно проводити з врахуванням функціонального призначення приміщення та професійних обов'язків працівника. Досить часто приміщення підприємства, яке є основним робочим місцем одного працівника, може бути допоміжним для іншого. Тому обов'язковим є розподіл території підприємства на окремі функціональні зони індивідуально для груп персоналу. Також необхідно розробити часовий регламент діяльності кожного працівника підприємства через визначення впливу відпрацьованого часу, продуктивних та непродуктивних простоїв на фонд оплати праці. Як наслідок, для працівників можливо розробляти часові інструкції виконання функціональних обов'язків, переміщення територією підприємства та роботи з дому. Регламентування часових параметрів роботи працівників сприяє уникненню надмірного скупчення працівників у приміщеннях підприємства, що сприятиме мінімізації біологічних загроз (особливо можливість інфікування COVID-19).

Корисним також є автоматизоване порівняння часових нормативів та показників фактично відпрацьованого часу. При понаднормовій роботі доцільно автоматично нараховувати додаткові виплати працівникам. У випадку фіксованої тривалості робочого дня доцільно застосовувати компенсаційні виплати за роботу у понаднормовий час. Аналогічно керівництвом підприємства за допомогою додаткових доплат до заробітної плати може стимулюватися дистанційне виконання функціональних обов'язків з дому. У такому випадку мінімізуються не лише біологічні ризики, але й скорочуються витрати на утримання персоналу.

Застосування калькуляційної одиниці «хвилина» доцільно розпочинати з другої години понаднормової праці. Оскільки працівник в перші хвилини після завершення робочого дня може витрачати час на міжособові комунікації, процедури особистої гігієни, недоцільно кваліфікувати затримку на робочому місці як роботу в понаднормовий час. Тому заохочувальні виплати доцільно виконувати за повну першу годину та наступні хвилини понаднормової продуктивної праці.

Моніторингу підлягає також праця персоналу у нічний час та у вихідні дні. Через співставлення актуального часу з присутністю працівників на робочому місці (дистанційним виконанням функціональних обов'язків з дому), у робочих приміщеннях та за обладнанням, доцільно автоматизовано нараховувати основну та додаткову заробітну плату.

Аналогічно можна здійснювати контроль виконання функціональних обов'язків з дому через перманентний моніторинг усіх операцій, що відбуваються з дистанційних робочих місць. Контролю підлягає час роботи працівника у спеціалізованому програмному забезпеченні, виконання маніпуляцій в Інтернет просторі, які передбачені його посадовими інструкціями. Час тривалих простоїв, отримання розважальної інформації, користування соціальними мережами і т.д. виключаються з фонду робочого часу працівника та заробітної плати.

На основі облікової інформації зі системи біометричної ідентифікації персоналу можна в електронному форматі заповнювати первинні

документи: табель обліку відпрацьованого часу, відомість нарахованої заробітної плати та інші. Розрахункові листки рекомендовано автоматично надсилати на робочі місця фахівців чи особисту електронну пошту з метою інформування про методику розрахунку заробітної плати та утримань з неї.

Факт формування розрахункових відомостей зі заробітної плати може запускати автоматичний процес її виплати. З попередньо встановленим часовим лагом після реєстрації в системі відомостей нарахованої заробітної плати доцільно формувати відповідні банківські документи. Після отримання електронних погоджень від посадових осіб, відповідальних за розрахункові транзакції, автоматизовано здійснюється відправка платіжних документів до виконавця через систему банківських комунікацій. Більш детально про методику грошових транзакцій та особливості їх обліку в умовах цифрової економіки розкрито у науковій праці [193]. Банк здійснює перерахунок коштів на особисті зарплатні рахунки (карткові проекти) працівників, що завершує цикл нарахування та виплати заробітної плати.

Окрім персоналу підприємства, інформацію про фонд робочого часу та заробітної плати з системи біометричної ідентифікації персоналу доцільно автоматизовано надсилати зацікавленим стейкхолдерам. Облікова інформація окрім внутрішніх цілей може використовуватися для: верифікації лікарняних листів при нарахуванні компенсації за умовами соціального та медичного страхування; формування узагальнених статистичних масивів даних про кількість працівників та розмір заробітної плати; перевірки достовірності нарахування податків й внесків у фонди соціального страхування тощо.

Систему біометричної ідентифікації осіб також рекомендовано використовувати для обліку витрат підприємства на утримання персоналу. До початку пандемії COVID-19 зростали витрати на соціальне, побутове та рекреаційне забезпечення працівників. На інноваційних підприємствах активно створювалися просторові зони спільного використання, до яких окрім коридорів, туалетів, ванних кімнат також можна віднести ігрові приміщення, лекційні аудиторії, зали засідань та нарад тощо. З

дистанційним та ізольованим виконанням функціональних обов'язків працівників структура витрат на утримання персоналу змінилася. Також некоректним є облік витрат на обслуговування приміщень для перебування працівників, які виконують функціональні обов'язки дистанційно. Враховуючи вільний доступ усіх працівників до спільних просторових зон, а також перенесення робочих місць деяких фахівців за межі підприємства, досить складно здійснювати ефективний розподіл витрат на утримання працівників між виробничими, адміністративними, збутовими чи іншими цілями.

На основі ідентифікації загальної кількості працівників різних напрямків діяльності, які фізично перебували у зонах спільного використання, доцільно автоматизовано розподіляти витрати на їх утримання між різними групами. Іншими словами, сукупні витрати на експлуатацію приміщень в кінці звітного періоду можна групувати пропорційно кількості відвідувачів виробничого, загальновиробничого, адміністративного, збутового та іншого персоналу за звітний період. Витрати на обслуговування працівників, які працюють за межами підприємства, не враховуються.

Інформація зі системи біометричної ідентифікації про кількість та посади працівників, які відвідали приміщення прийому їжу, є підставою для автоматизованого обліку витрат на утримання персоналу. Витрати на харчування у столових, барах, кафе, яке повністю або частково фінансується за рахунок підприємства, доцільно автоматизовано розподіляти на декілька груп за напрямками діяльності. Після завершення робочої зміни чи календарного дня сукупні витрати на харчування рекомендовано класифікувати на різні види пропорційно кількості відвідувачів та їх посад. З використанням технології біометрії забезпечується достовірний облік витрат без необхідності фіктивного розподілу між усіма працівниками (у тому числі, які перебувають удома) або віднесення до складу лише однієї групи (статті) витрат.

Інформацію зі системи біометричної ідентифікації про відпрацьований працівниками виробництва час та заробітну плату можна також використовувати як оптимальну базу для розподілу

загальновиробничих витрат. В обліковій практиці підприємств проблемним моментом є необхідність нарахування заробітної плати працівникам, які одночасно можуть працювати на декількох посадах, в різних виробничих підрозділах над виготовленням декількох видів продукції тощо. Як паралельне, так і дистанційне (з дому) виконання персоналом функціональних обов'язків негативно впливає на достовірність розподілу загальновиробничих витрат пропорційно заробітній платі виробничого персоналу. Натомість біометрична ідентифікація працівників з фіксацію виконання ними функціональних обов'язків винятково виробничого характеру сприяє оптимізації обліку та розподілу загальновиробничих витрат на підприємстві. Аналогічно автоматизації підлягають усі витрати, які пов'язані з утриманням та діяльністю працівників на підприємстві з використанням інформації з автоматизованої системи біометричної ідентифікації персоналу.

2.5. Комплексне використання технології стільникового зв'язку 6G в обліку витрат діяльності та кібербезпеці

Зростання мобільності населення та дистанційне виконання посадових обов'язків в період пандемії COVID-19 та військових дій формує нові вимоги до швидкості передачі даних у мережі Інтернет. Сучасні технології Інтернету речей, блокчейн, адаптивного аудіо та відеострімінгу ґрунтуються на використанні високошвидкісних безпровідних електронних комунікацій. Підтримка безпровідного стільникового зв'язку імплементується у сучасні носимі, побутові та промислові технологічні пристрої. Збір даних та управління функціональними процесами відбувається дистанційно в перманентному режимі через мережу Інтернет. Сучасні технології стільникових мереж 4G не здатні забезпечити потреби користувачів у великих масивах даних з мінімальним часовим лагом, що стримує цифровізацію соціально-господарських процесів.

Активно ведуться теоретичні дослідження та впроваджуються прикладні розробки щодо використання стільникових мереж п’ятого покоління. Технологія стільникового зв’язку 5G уможливлює повну трансляцію соціально-економічних розрахунків в хмарне середовище, використання технології блокчейн на усіх технічних пристроях, об’єднанням технологічного обладнання у єдину виробничу інформаційну мережу тощо. Натомість, господарське використання напрацювань у сфері штучного інтелекту, тотальної віртуалізації комунікацій, безпілотності та автопілотності транспортних засобів, під’єднання до Інтернету усіх технічних пристроїв визначає досяжний горизонт нової шостої генерації стільникового зв’язку, функціонуванню якої загрожують принципово нові кіберризики.

Проблематика забезпечення ефективного кіберзахисту в умовах використання стільникового зв’язку 6G є предметом наукового пошуку багатьох науковців. Lu Yang [118] дослідив історичний розвиток кіберзагроз стільникового зв’язку від 1G до 5G, що дало змогу визначити тренди забезпечення кіберзахисту в умовах технології 6G. Продовжили дослідження Porambage Pawani та інші [145], які спрогнозували проблемні аспекти використання потенційних технологій у стільникових мережах 6G, таких як: технологія розподіленого реєстру (DLT), захист фізичного рівня, розподілений штучний інтелект, THz й квантові обчислення та запропонували способи забезпечення кібербезпеки підприємств. Huang Russell та Turner Grant [96] дослідили досвід Великобританії щодо забезпечення кіберзахисту від інформаційного шпіонажу корпорації Huawei з використанням технології стільникового зв’язку 5G та спрогнозували можливі загрози 6G для кібербезпеки. Zhang Junwei та інші [199] розробили схему децентралізованого інформаційного обміну з використанням стільникового зв’язку 6G для реалізації краудсорсингу (передачі виробничих та інформаційних функцій невизначеному колу осіб), що формує нові вимоги до кібербезпеки.

Значна увага приділяється удосконаленню понятійного апарату наукових досліджень у частині забезпечення кіберзахисту у сфері 6G. Зокрема, Popovski Petar та інші [144] провели ґрунтовні дослідження щодо розвитку стільникових мереж 6G та пов'язаних понять «одночасності», «присутності» та «причинності», які є базовими категорія у забезпеченні інформаційної безпеки користувачів телекомунікаційних послуг. Термінологічні дослідження також провели Ylianttila Mika та інші [188] і Wang Minghao та інші [183], які обґрунтували позиціонування понять «довіри», «безпеки» та «конфіденційності» у контексті створення надійного стільникового зв'язку 6G, що передбачає розвиток мультидисциплінарних технологій, методик регулювання, техноекономіки, політики та етики.

У науковому просторі наявні різносторонні дослідження предметного використання технологій стільникового зв'язку 6G у поєднанні з кібербезпекою суб'єктів господарювання. Наприклад, Siriwardhana Yushan та інші [167] обґрунтували значний рівень проникнення механізмів штучного інтелекту у функціонування 6G, що створює значні кіберризики у діяльності операторів та користувачів стільникового зв'язку. Водночас науковці звертають увагу, що штучний інтелект здатний уникати та попереджувати прояв кіберзагроз у функціонуванні суб'єктів господарювання. Інтеграція технологій блокчейн та 6G, на думку Khan Ali Hussain та інші [104], створює можливості для ефективного захисту інформації через децентралізацію стільникових мереж та розподіленого доступу до баз даних. Науковці дослідили різні варіанти поєднання технології блокчейн з напрямками використання стільникового зв'язку 6G, що сприяє оптимізації кіберзахисту. Hoschek Miloslav [95] пояснив вплив квантумної кібербезпеки на функціонування критичноважливої інфраструктури, що функціонує на основі використання стільникових мереж 5G та, в перспективі, 6G. Аналогічні дослідження провели Al-Mohammed H. та Yaacoub E. [50] щодо перспектив розвитку технології Інтернету речей в еру стільникового зв'язку 6G, що потребує використання квантумних обчислень та комунікацій.

Узагальнення наукового доробку авторів дає змогу ідентифікувати кіберризики, що загрожують стільниковим мережам 6G: атаки з використанням штучного інтелекту, попередньо невідомі вразливості «нульового дня», ризики на основі квантумних обчислень, атаки з використанням швидкого (ТераГерцового) обладнання, фізичні атаки з метою прослуховування телефонії тощо, що потребує удосконалення методів кіберзахисту та мікро-рівні (рис. 2.9).

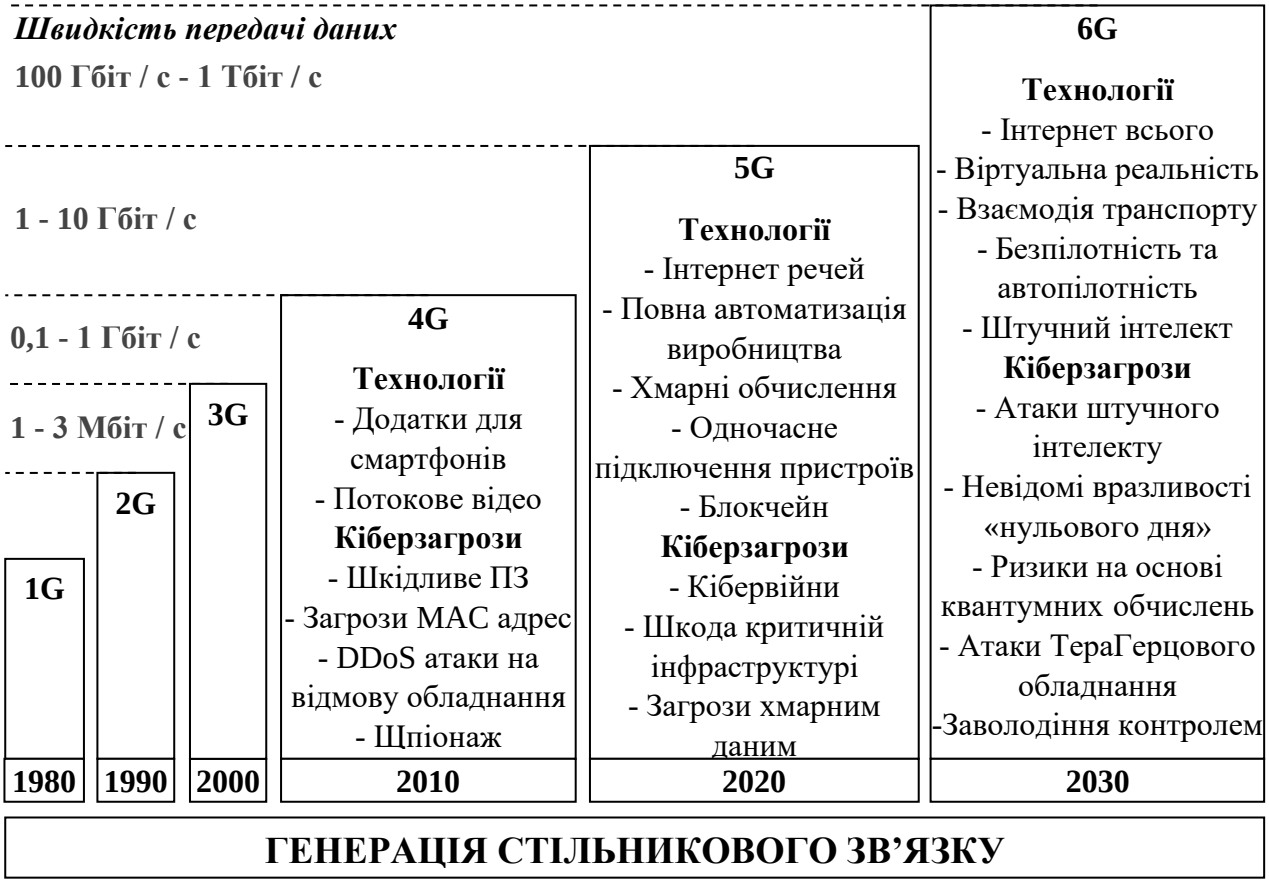


Рис. 2.9. Розвиток стільникових мереж мобільних комунікацій

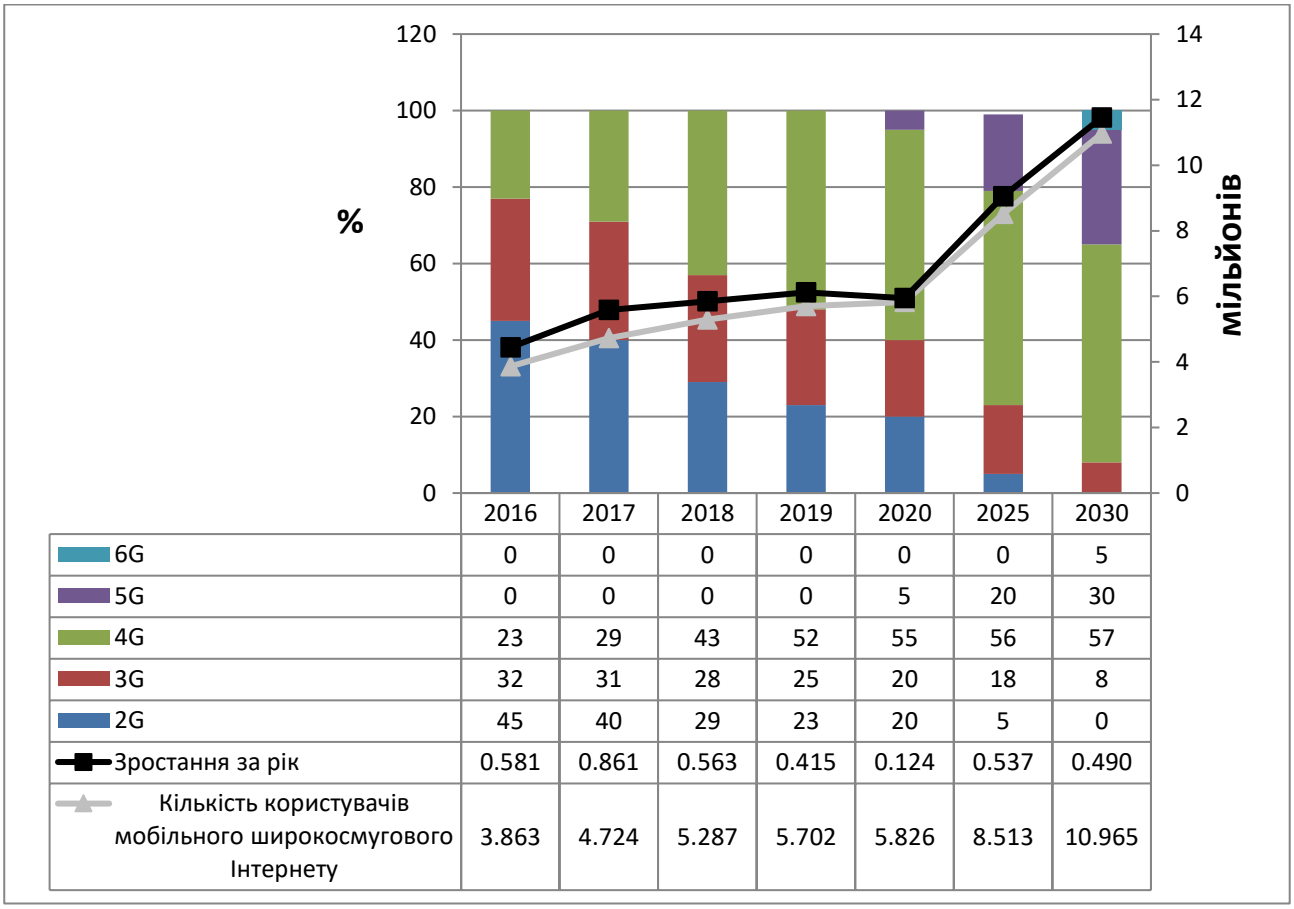
Джерело: сформовано автором на основі [118]

У мережах стільникового зв'язку попередніх поколінь за кіберзахист інформації відповідальність несуть телекомунікаційні компанії. Оператори стільникових мереж інвестують значні кошти в програмно-технічне забезпечення систем кібербезпеки, збільшують штат працівників безпекової служби, здійснюють розслідування кіберінцидентів. В умовах

імплементації технології 6G на мікро-рівні функції кіберзахисту частково передаються керівництву суб'єктів господарювання.

У менеджменту виникає необхідність в забезпечення кібербзепеки телекомунікаційного обладнання, що встановлене у приміщеннях (на території) підприємства. Прямий інформаційний обмін у рамках стільникового зв'язку 6G перебуває у повній відповідальності працівників підприємства, а тому потребує додаткових заходів щодо реалізації ефективного кіберзахисту.

Наявність значних кіберризиків використання технології стільникового зв'язку нових поколінь є перешкодою до їхнього масового застосування, що можливо прослідкувати з рис. 2.10.



	2016	2017	2018	2019	2020	2025	2030
6G	0	0	0	0	0	0	5
5G	0	0	0	0	5	20	30
4G	23	29	43	52	55	56	57
3G	32	31	28	25	20	18	8
2G	45	40	29	23	20	5	0
Зростання за рік	0.581	0.861	0.563	0.415	0.124	0.537	0.490
Кількість користувачів мобільного широкосмугового Інтернету	3.863	4.724	5.287	5.702	5.826	8.513	10.965

Рис. 2.10. Темпи розповсюдження пристроїв стільникового зв'язку за генераціями (2G-6G)

Джерело: визначено на основі [82; 124; 125]; показник для 2030 р. розрахований на основі прогнозування даних

Щороку збільшується кількість пристроїв, під'єднаних до стільникового зв'язку (з 3,863 мільйонів у 2016 році до 5,826 мільйонів у 2020 році). Перманентне зростання популярності стільникових пристроїв частково пояснюється розвитком нових поколінь стільникового зв'язку 4G (частка у 2020 р. – 55%) та 5G (частка у 2020 р. - 5%). Але слід врахувати недостатні майбутні темпи впровадження стільникового зв'язку п'ятого та шостого поколінь. Зокрема, якщо частка популярності 4G за 5 років збільшилася на 32%, то прогнозований ріст використання технології 5G у 2020-2025 рр. лише 15% на фоні популяризації технології Інтернету речей, під'єднаних до стільникового Інтернету. Аналогічні показники очікуються й для використання технології 6G.

Ключовою характеристикою технологій 5G та 6G є достовірне визначення місця перебування абонента стільникової мережі. Аналогічно технології глобального супутникового позиціонування (GPS) можуть бути використані для ідентифікації просторового розташування смартфону та, відповідно, його власника. Якщо GPS-навігація забезпечує формування двовимірної інформації про розташування і переміщення підконтрольного об'єкта, то стільникові мережі сприяють трохвимірному позиціонуванню. Іншими словами, на основі технологій 5G та 6G можливо визначати висоту перебування стільникового апарату у відкритому просторі або поверх будівлі – у закритому.

Іншою важливою можливістю стільникових мереж нового покоління є прямий інформаційний обмін між технічними пристроями. Без залучення базових станцій смартфони здатні обмінюватися даними з іншими пристроями, що мають доступ до стільникового зв'язку. Прямі комунікації забезпечують отримання оперативних й повних даних, що є цінним інформаційним ресурсом для цілей бухгалтерського обліку та управління. Функціональні можливості використання технології 6G у частині автоматизації обробки та кіберзахисту облікової інформації відображено на рис. 2.11.

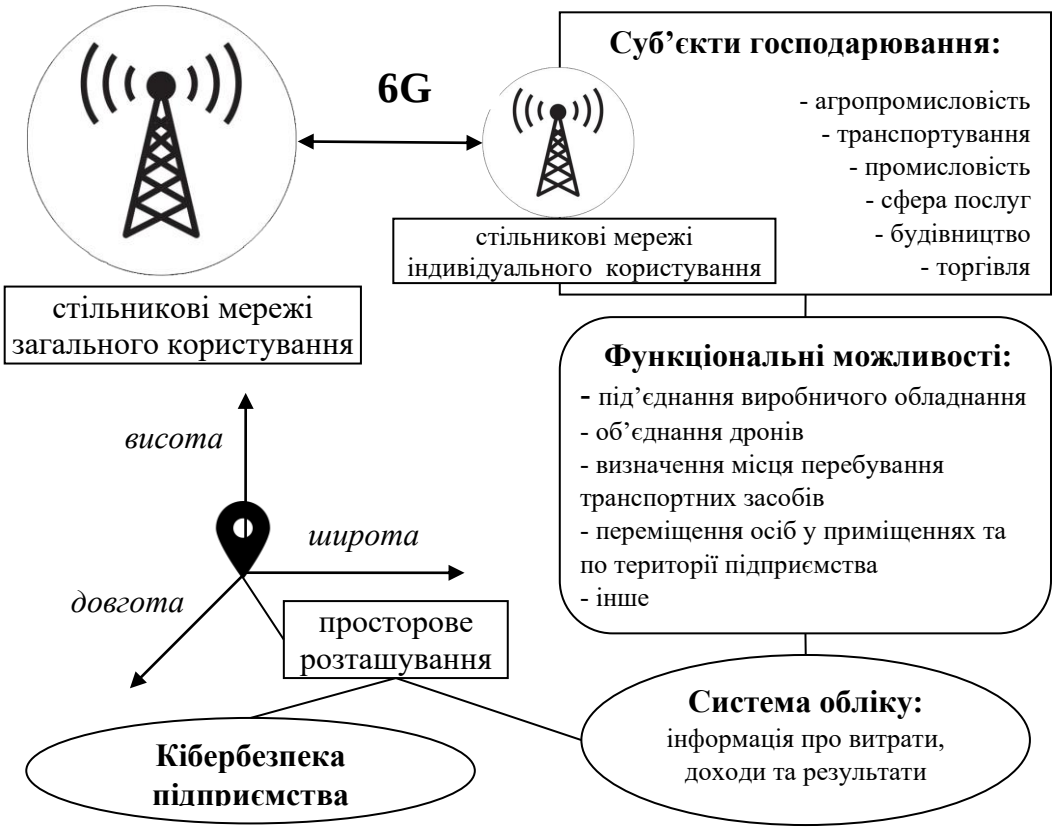


Рис. 2.11. Використання стільникових мереж 6G для цілей обліку та кібербезпеки підприємств

Джерело: сформовано автором

Використання стільникового зв'язку 6G розширює функціональні можливості технології GPS у моніторингу комерційного функціонування транспортних засобів. Окрім інформації про маршрути пересування та зупинки автотранспорту, на основі технології 6G можливо отримати інформацію про витрати палива, факти завантаження (розвантаження), непродуктивні простої, поломки, необхідність технічного обслуговування чи ремонту, порушення правил дорожнього руху тощо, що може бути корисною для цілей бухгалтерського обліку та кіберзахисту.

Зокрема, після завершення поїздки доцільно використовувати дані, отримані з використанням технології 6G, для обліку паливо-мастильних матеріалів. Для кожного факту переміщення транспортного засобу рекомендовано визначати витрати палива (електроенергії) з метою достовірної ідентифікації собівартості транспортних послуг. Інформація про пройдену автотранспортом відстань у кілометрах є

малоінформативною для оперативного та достовірного обліку транспортних витрат. Різний стиль водіння транспортних засобів, рельєф місцевості та стан доріг, вага перевезеного вантажу значно впливає на витрати палива та, особливо, електроенергії для електромобілів. Тому лише на фактичні витрати палива (електроенергії), надані з використанням технології 6G, а не на інформацію про кілометраж пробігу автотранспорту, доцільно орієнтування при автоматизації обліку транспортних послуг.

Інформацію про своєчасно виявлені факти непродуктивного використання транспортних засобів доцільно використовувати для обліку та контролю діяльності транспортних підприємств. Після ідентифікації нецільового використання або незапланованого простою транспортних засобів у робочий час, отримання штрафів за порушення правил дорожнього руху можливо одномоментно визначати відповідальних за порушення працівників із відображенням в обліку відшкодування завданих збитків.

Окрім традиційного захисту від крадіжок транспортних засобів стільниковий зв'язок 6G може використовуватися для організації автопілотного дорожнього руху. Через механізми миттєвої взаємодії на основі стільникових мереж 6G транспортні засоби можуть уникати зіткнень та виконувати правила дорожнього руху. В такому випадку важливим є забезпечення належного кіберзахисту автотранспорту для запобігання несанкціонованого доступу зловмисників. Використовуючи стільникові мережі, треті особи можуть отримати дистанційний контроль над транспортними засобами для вчинення подальших протиправних дій. Отже, рекомендованою є розробка новітніх протоколів кіберзахисту стільникових комунікацій в поєднанні з перманентним контролем дотримання встановлених маршрутів пересування транспортних засобів та правил дорожнього руху.

Разом з організацією автопілотного пересування автотранспорту з використанням стільникового зв’язку 6G можливим є забезпечення інформаційного зв’язку з безпілотними літальними апаратами (дронами). З використанням систем штучного інтелекту доцільно об’єднувати дрони в рої з метою збору інформації для цілей обліку та кібербезпеки

будівельних та аграрних підприємств. Об’єднання (рої) безпілотних літальних апаратів здатні здійснювати моніторинг господарської діяльності у цілодобовому режимі без прямої участі працівників підприємства. Після отримання з дрону сигналу про низький рівень заряду акумулятора на заміну відправляється новий безпілотний літальний апарат. Попередній дрон повертається для поновлення запасу електроенергії, що є основою перманентної ротаційної експлуатації безпілотних літальних апаратів.

На основі даних про стан виконання будівельних робіт доцільно здійснювати автоматизований облік витрат й доходів відповідно до ступеня завершеності будівництва, що обґрунтовується будівельним контрактом. На основі аеровізуальної ідентифікації ступеня виконання будівельних робіт (зведення цілої будівлі, окремої частини чи поверху (секції)) можливо достовірно визначати собівартість наданих будівельних послуг. Замовнику будівництва певних об’єктів може повідомлятися проміжна його вартість відповідно до будівельного контракту. Відповідно у системі обліку доцільно автоматизовано фіксувати понесені витрати, отримані доходи й визначений фінансовий результат від надання будівельних послуг за довільний проміжок часу. За фактом виконання певного етапу будівництва на основі моніторингу дронами будівельних робіт усі облікові процедури можуть виконуватися щоденно, що забезпечує своєчасність та оперативність обліку й контролю.

Аналогічно дрони, керовані через стільникову мережу 6G, здатні здійснювати аеровізуальне спостереження за процесом виконання аграрних робіт. Зібрана інформація про обробку ґрунту, посівний процес, біологічні перетворення рослин, збір урожаю доцільно використовувати для обліку витрат аграрних підприємств. На основі фото та відеоматеріалів можливо автоматизовано визначати потребу в паливно-матеріальних запасах, посівному матеріалі, засобах захисту рослин, мінеральних добривах тощо з автоматизованим фіксуванням у бухгалтерському обліку. Оперативний облік витрат матеріалів адитивним способом забезпечує формування проміжної собівартості аграрної продукції. Як наслідок, ще до завершення виробничого циклу можливо

прогнозувати повну собівартість та планувати продажну вартість продукції аграрного виробництва.

Безпілотні літальні апарати здатні в автоматизованому режимі виявляти порушників периметру території та повітряного простору. На основі візуального розпізнавання обличь і порівняння з базою даних зображень персоналу підприємства, можливе виявлення сторонніх осіб, які не мають права перебувати в зоні безпекового контролю. Окрім штатних працівників у базу даних персональної інформації вносяться візуальні образи обличь третіх осіб, які виконують періодичні роботи (надають послуги) або є візитерами, що отримують разові права доступу.

Також безпілотні літальні апарати можуть виявляти присутність інших сторонніх дронів. З масових розвитком малої (персональної) авіації у розпорядженні зловмисників, конкурентів, ЗМІ та інших осіб з’являються засоби аеровізуального шпіонажу. У випадку виявлення порушників територіального та повітряного простору дрони повідомляють безпекові підрозділи підприємства для призупинення протиправних дій.

Стільниковий зв'язок 6G може імплементовуватися в будь-яке виробниче обладнання з метою оперативної передачі інформації про виробництво. Незалежно від просторового розташування засобів виробництва продукції можливий автоматизований збір параметрів виробничого процесу. Технологічні дані з датчиків, якими обладнані основні засоби підприємства, доцільно використовувати для автоматизованого обліку виробничих витрат. Виробниче обладнання здатне фіксувати кількість та якість витрачених матеріальних цінностей та електроенергії (води, газу тощо) у процесі виробництва продукції (робіт, послуг). Усі факти використання предметів праці доцільно автоматизовано фіксувати в бухгалтерському обліку. З використанням методики неповного калькулювання собівартості доцільно оперативно визначати усі прямі виробничі витрати. Калькулювання відбувається на перманентній основі, коли для кожної одиниці готової продукції можливо достовірно визначати собівартість. У керівництва підприємства з’являється можливість точного пооб’єктного визначення собівартості

продукції, що дає змогу одномоментно коригувати вартість реалізації для кожного індивідуального замовлення та покупця.

У функціонуванні виробничого обладнання доцільно передбачити механізм ідентифікації осіб, які перебувають поруч. Особа, яка відвідувала робоче місце та не є штатним працівником, може ідентифікуватися як порушник безпекового режиму. У випадку отримання бракованої продукції, крадіжки сировини, понаднормове витрачання ресурсів можливо визначити підозрюваних осіб. Про усі факти порушень автоматично повідомляється безпековий підрозділ підприємства.

На основі інформації про відвідування певних видів приміщень також рекомендовано достовірно визначати орендну плату для операторів торгових площ. Залежно від кількості осіб, які відвідали торгові зали орендаря, змінюється розмір оренди. В кінці місяця доцільно розраховувати та відображати в обліку орендну плату, яка встановлюється пропорційно кількості відвідувачів та площі, яка передана орендарю. Кількісний варіант ціноутворення є корисним для операторів орендних площ, що дає змогу ефективно врахувати витрати на обслуговування відвідувачами не лише торгівельних площ, але й зон загального використання. До таких приміщень відносяться коридори, туалети, сходи, ескалатори, лаундж-зони тощо.

Витрати на обслуговування приміщень загального призначення (обігрів, кондиціонування, прибирання, поточний ремонт тощо) оператори торгівельних площ в основному напряму закладають у вартість орендної плати, що порушує фундаментальні облікові принципи. Натомість ціноутворення з врахуванням кількості відвідувачів забезпечує справедливий розподіл таких витрат. Окрім торгівельних закладів облік витрат на основі кількості відвідувачів доцільно використовувати для підприємств громадського харчування, туризму, транспортного обслуговування пасажирів.

За аналогічною методикою можливо визначати ефективність зовнішньої реклами та функціонування виставкових вітрин в торгівельних закладах. З використанням технології 6G керівництво підприємства отримує інформацію про популярні маршрути пересування відвідувачів

торгівельних закладів. На основі інформації про кількість та тривалість зупинки відвідувачів біля рекламної вивіски чи вітрини рекомендовано визначати популярність та дієвість маркетингових заходів. Відповідно, із зростанням популярності певних місць розміщення зовнішньої реклами чи продукції (товарів) може збільшуватися вартість оренди рекламної та торгівельної площі. Для замовників рекламних вивісок вартість послуги визначається індивідуально з чіткою прив'язкою до потенційної кількості осіб, які можуть бути споживачами маркетингових заходів.

З іншого боку доцільно здійснювати моніторинг популярності певного виду чи типу продукції (товарів), які становлять інтерес у покупців, але з нез'ясованих причин не продаються. Іншими словами, з'ясування потребує підвищення уваги то матеріальних цінностей, що не завершується фактом їхньої реалізації. Для такої продукції (товарів) необхідна зміна цінової, збутової чи мерчандайзингової політики.

Досить часто організаційно складно забезпечити відеоспостереження та автоматизований контроль пропуску працівників на територію в умовах значного потоку людей чи великої площі моніторингу. З використанням технології 6G доступним є контроль переміщення осіб територією підприємства. У системі кібербезпеки підприємства доцільно фіксувати факти потрапляння сторонніх осіб, що користуються стільниковим зв'язком, у приміщення чи окремі зони території з обмеженим доступом. Якщо порушник інформаційного чи територіального режиму оперативно визначається системою кібербезпеки, можливо запобігти кіберзлочинам.

У випадку запізнілого виявлення втратити матеріальних чи інформаційних ресурсів доцільно визначити осіб, причинених до правопорушення. На основі ідентифікації переліку осіб, які територіально перебували поруч місця інциденту у певний проміжок часу, можливо визначати правопорушників на основі виявлення індивідуального номера стільникового зв'язку. У процесі подальших слідчих дій доводиться причетність абонентів стільникового зв'язку до кіберінциденту. Узагальнені можливості, що досліджені у статті, та виклики технології стільникового зв'язку шостого покоління наведені у табл. 2.3.

Таблиця 2.3

Можливості та виклики технологій, реалізованих на основі стільникового зв’язку 6G, для цілей кібербезпеки

Технології 6G	**Можливості для кіберзахисту**	**Виклики для кіберзахисту**
Позиціонування	Моніторинг переміщення осіб територією, приміщеннями підприємства. Ідентифікація правопорушників інформаційного режиму.	Етичність надмірного контролю за переміщенням абонентів стільникового зв’язку. Запобігання потрапляння особистих даних абонентів до сторонніх осіб.
Автопілотність / безпілотність	Контроль за переміщенням та функціонуванням комерційного транспорту. Координування безпілотних літальних апаратів у процесі аеровізуального спостереження.	Захист від отримання фізичного контролю сторонніми особами над транспортними засобами чи дронами.
Інтернету речей	Підключення усього виробничого обладнання до Інтернету на принципах технології Інтернету речей для оперативного автоматичного (без працівників) збору та передачі даних	Запобігання викривлень та викрадень інформації у момент її збору та передачі
Блокчейн	Забезпечення розподіленого доступу та зберігання даних.	Неможливість контролю з боку державних інституцій.
Квантова безпека	Незламне шифрування даних у процесі передачі	Нестача існуючої обчислювальної потужності в операторів стільникового зв’язку. Складність стандартизації.
Штучний інтелект	Автономне управління системою безпеки. Оптимізоване забезпечення безпеки.	Проблемна масштабованість. Складність автоматичного визначення правопорушників та інформування служби кібербезпеки. Необхідність захисту обчислювальної інфраструктури на мікро-рівні.

Джерело: систематизовано автором

Практичне втілення поданих у статті розробок щодо використання технологій стільникового зв’язку 6G сприятиме достовірному калькулюванню собівартості продукції (робіт, послуг) та обліку виробничих витрат виробничої, сільськогосподарської, будівельної, торгівельної діяльності у поєднанні із забезпечення ефективного кіберзахисту підприємств у частині попередження та виявлення порушників інформаційного та територіального безпекового режиму.

РОЗДІЛ 3. ОРГАНІЗАЦІЯ ОБЛІКУ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ПІДПРИЄМСТВ

3.1. Кібербезпекові регламенти облікової політики підприємства

Основним регламентуючим документом у сфері інформаційного кругообігу на мікрорівні є облікова політика підприємства. Вона є одним з перших нормативно-правових актів, що формується при створенні будь-якого суб'єкта господарювання, та орієнтиром для фахівців з обліку й управління у реалізації облікових принципів і підготовці звітності. Документ про облікову політику є домінантним у нормативно-правовому регулюванні обліку, оскільки на нього посилаються інші внутрішні регламенти. В обліковій політиці зазначаються умови функціонування, що випливають з організаційно-правової форми, галузі діяльності, розміру бізнесу і т.д. Важливого значення в регламентування інформаційних процесів має відображення організаційної структури підприємства, що безпосередньо впливає та порядок обробки облікової інформації та формування звітних показників.

Облікова політика використовується у доведенні контролюючими інституціями протиправних дій облікового та управлінського персоналу підприємства. У цьому регламентуючому документі містяться непорушні інструкції, які визначають єдиний з варіативних методів та способів обробки облікової інформації. Все більше підприємств регламентують не тільки методику фінансового обліку та пов'язаних з ним податкових розрахунків, але й особливості управлінського обліку. В обліковій політиці з управлінського обліку зазначаються центри відповідальності й центри обліку витрат, методика калькулювання та визначення собівартості продукції, порядок формування управлінської звітності тощо.

Тому із ускладненням соціально-економічних процесів, виникненням нових об'єктів обліку, діджиталізацією економіки виникає необхідність в удосконаленні облікової політики. Подальший розвиток інституту регламентації обліку потребує розширення предметного поля облікової

політики. В документі про облікову політику підприємства доцільно передбачити безпекові аспекти обробки облікової інформації, формування і подання звітності стейкхолдерам.

Кібербезпеку в системі обліку Цаль-Цалко Ю.С. та Мороз Ю.Ю. визначають як захищеність інформаційної системи підприємства від внутрішніх і зовнішніх загроз, тобто захист підприємства, його кадрового і інтелектуального потенціалу, інформації, технологій, прибутку, доданої та ринкової вартості підприємства, який забезпечується системою заходів спеціального правового, економічного, організаційного, інформаційно-технічного і соціального характеру, що впливають на формування облікової політики [23, с. 9]. Одним з перших науковців, хто пояснив вплив інформаційного суспільства та цифрової економіки на формування і впровадження облікової політики, є Пушкар М.С., Щирба М.Т. [32].

Перелік складових облікової політики у розрізі її об'єктів, суб'єктів, мети і завдань, рівнів регулювання надав у науковій праці Герасимович І.А. [9]. Проведене дослідження дає змогу сформувати комплексне розуміння облікової політки та її значення для функціонування підприємства в умовах трансформації та цифровізації соціально-економічних процесів. Кафка С. запропонувала інформаційно підпорядкувати різні внутрішні регламенти (графіки документообіг, проекти автоматизації обліку, посадові інструкції облікових працівників) обліковій політиці підприємства [101].

Продовжили дослідження Alibha Salim та інші [48], які обґрунтували вплив облікової політики на помилки в обробці облікової інформації та формуванні звітності. На думку авторів, існує чітка відмінність між помилками в обробці інформації та змінами в облікових принципах чи методах оцінки. Необхідність розширення положень облікової політки (Облікова політика 2.0) дослідив Kim Jihyun [105], виходячи з трансформації законодавства США.

Також Harrast Steven [92] запропонував перелік положень щодо роботизації виробничих процесів та повної автоматизації інформаційних процесів, які доцільно відображати в обліковій політиці підприємства. Лаговська О. та Лоскоріх Г. [112] пояснили відмінність у формуванні

облікової політики ІТ підприємств від інших галузей економіки. Науковцями розроблено схему облікової політики для підприємств, які функціонують у сфері ІТ бізнесу. Drokina N. і Kaipova Gulnara [74], визначаючи контент облікової політики, значну увагу приділили положенням автоматизованого обліку. На думку науковців, методику автоматизованої обробки облікової інформації доцільно відображати в документі про облікову політику підприємства.

Проте науковці акцентують дослідження на програмно-технічних положеннях облікової політики щодо кіберзахисту підприємства. Проте, організаційні аспекти кібербезпеки залишаються поза увагою науковців, що і визначає актуальність досліджень у напрямку безпекових компонентів облікової політики підприємства. Як наслідок, в обліковій політиці підприємства доцільно врахувати безпекові положення для організації належного кіберзахисту інформаційної системи підприємства. Безпекові регламенти є сукупністю вимог, правил, обмежень, порядків дій та відповідальності персоналу щодо обробки та передачі облікової інформації з метою досягнення і підтримки стану максимальної інформаційної та кібербезпеки підприємства.

Інформаційна безпека підприємства безпосередньо залежить від ефективної облікової політики підприємства. Чітка регламентація в обліковій політиці дій фахівці з обліку та управління щодо збору, реєстрації, обробки та передачі інформації значно мінімізує інформаційні загрози. У випадку неналежної уваги керівництва підприємства до комунікаційних зв'язків у внутрішньому та зовнішньому інформаційному середовищі появляються можливості до маніпулювання обліковими даними та їх викрадення з метою завдання збитків підприємству чи одержання неправомірної вигоди. «Слабкі місця» в інформаційній цілісності підприємства можуть бути використані третіми особами задля одержання доступу до комерційної таємниці підприємства. Інформаційна безпека обов'язково повинна бути комплексною, враховувати усі комунікаційні канали та зв'язки між учасникам облікового процесу, передбачати реалізацію правових, технічних, програмних та організаційних заходів, що регламентуються обліковою політикою підприємства.

Якщо суб’єкт господарювання характеризується наявністю значної кількості працівників, складністю структури управління, значними обсягами господарської діяльності, можливий варіант із формування окремих регламентуючих документів за напрямками забезпечення кібербезпеки з реалізацією інформаційної сумісності та єдності з обліковою політикою підприємства. Облікова політика в такому випадку може бути інтегратором усіх внутрішніх регламентів щодо забезпечення кібербезпеки. Завдяки системі бухгалтерського обліку може формуватися внутрішнє правове поле організації та методики кіберзахисту, що разом становить облікову політику підприємства. Інформаційна схема безпекових положень, що зафіксовані у внутрішніх нормативних документах та обліковій політиці, подано на рис. 3.1.

Рис. 3.1. Безпекові регламенти в обліковій політиці підприємства та внутрішніх нормативних документах

Джерело: сформовано автором

Основою комплексної системи інформаційної безпеки на підприємстві є повний розподіл прав доступу до облікової інформації. Усім обліковим та управлінським працівникам залежно від посади та ієрархічного рівня в системі управління доцільно обмежити фізичний доступ до баз даних через механізм індивідуальних цифрових підписів. З метою забезпечення розподіленого доступу до облікової інформації необхідно на підприємстві розробити Положення про комерційну таємницю. На думку Боримської К.П. та Кінзерської Н. В., у положенні необхідно чітко зазначити, які відомості є комерційною таємницею, порядок віднесення їх до таких, умови зберігання, а також працівників підприємства, які можуть передавати закриті відомості представникам державних організацій [5, с.17].

Увесь персонал підприємства необхідно розділити на рівні прав доступу. У Положенні про комерційну таємницю доцільно розмістити таблицю відповідностей кожного працівника індивідуальному безпековому рівню. Обсяг наданої інформації має бути достатній для виконання функціональних обов'язків або прийняття ефективних управлінських рішень. У посадових інструкціях кожного працівника зазначається рівень допуску до комерційної таємниці та відповідальність за її розголошення. Як наслідок, облікова інформація обмежується для облікових та управлінських фахівців лише сферою їх прямих функціональних повноважень. При зростанні ієрархічного рівня управління збільшується і масив доступної для ознайомлення облікової інформації.

Обов'язково в обліковій політиці підприємства необхідно зазначати термін дії повноважень з допуску працівників до комерційної таємниці. Тривалість дії прав доступу прямо пропорційна рівню в ієрархії управління. Для працівників нижчого кваліфікаційного рівня необхідно суттєво скоротити календарний час та обсяг доступу до облікової інформації. Лише із зростанням стажу та професійних навичок доцільно збільшувати рівень інформаційної довіри до особи. Коригування часового допуску до комерційної таємниці забезпечить уникнення витоку

конфіденційних облікових даних через високу плинність кадрів чи тимчасово прийнятих на роботу агентів інформаційних зловмисників.

З метою недопущення сторонніх осіб до території підприємства використовується автоматизована система пропускного режиму. Рекомендовано обладнати усі приміщення підприємства технічними пристроями стеження. Подібно до функціонування системи доступу персоналу до облікової інформації доцільно організувати контроль за переміщенням працівників по території підприємства. В обліковій політиці необхідно передбачити класифікацію приміщень за правом допуску різних груп працівників. Завдяки системі автоматизованого пропускного режиму забезпечується контроль за несанкціонованим пересуванням персоналу. Забороняється прохід осіб до приміщень, які не відносяться до прямої їх компетенції та не призначені для виконання функціональних повноважень.

Також доцільно здійснювати контроль за доступом працівників до комп'ютерно-комунікаційної техніки. Комп'ютерна, телекомунікаційна та мережева системи належать підприємству, що вимагає використання її лише для виконання робочих завдань. Повністю заборонити персоналу використовувати програмно-технічне забезпечення в особистих цілять досить складно. Доцільно визначити в обліковій політиці порядок використання технічної та програмної інфраструктури підприємства з метою недопущення витоку конфіденційної інформації через несанкціоновані інформаційні сервіси. Тому необхідно заборонити доступ з робочих комп'ютерів до певного програмного забезпечення, веб-ресурсів та електронної пошти, що можуть бути використані зловмисниками для порушення інформаційної безпеки суб'єкта господарювання.

В додатковому внутрішньому регламенті необхідно передбачити перелік усього програмно-технічного забезпечення в розрізі прав доступу, яким може користуватися персонал підприємства. В документі «Політика управління доступом до програмно-технічного забезпечення» доцільно вказати на заборону: змінювати і копіювати файли, що належать іншим користувачам; встановлювати на комп'ютерах і в мережі стороннє

програмне забезпечення; пересилати електронною поштою будь-які документи іншим особам і організаціям; розміщувати особисті оголошення, клопотання, рекламні пропозиції тощо [22, с.318]. Обов'язково рекомендовано зазначити про можливість моніторингу та перевірки керівництвом підприємства змісту усієї інформації, яка відправляється з технічних пристроїв та комп'ютерних програм суб'єкта господарювання.

Система розподіленого доступу реалізується через механізм цифрових підписів. Кожному працівнику надається особистий електронних ключ, який доповнюється логіном та паролем. Цифровий ключ вводиться до програмного забезпечення працівника на всіх технічних пристроях виконання функціональних обов'язків. Персональні комп'ютери та мобільні пристрої можуть бути використані персоналом на території підприємства та поза його межами. Цифровий ключ є виключно персоналізований з метою ідентифікації кожної особи, відповідальної за реалізацію інформаційних процедур. Завдяки системі цифрових підписів можна здійснювати контроль за всіма інформаційними ресурсами та технічними пристроями, з якими мав справу обліковий чи управлінський фахівець. Рекомендовано прийняти на підприємстві Положення про застосування цифрових підписів, яким регламентується процес присвоєння та використання ключів доступу до облікової інформації.

Система електронних ключів активно використовується з метою захисту та ідентифікації інформаційних комунікацій з фіскальною службою країни. Тому більшість підприємств уже мають достатню інфраструктуру для використання цифрових підписів в інформаційних процесах. Рекомендовано доповнити існуючу систему автентифікації посадових осіб через обов'язкове присвоєння усім обліковим та управлінським працівникам ідентифікованих електронних ключів. Цифрові підписі ідентифікують працівника в процесі внутрішніх та зовнішніх комунікацій.

Для зовнішніх інформаційних зв'язків важливо вказувати обрані комунікаційні канали. З метою недопущення викрадення конфіденційних даних важливо регламентувати інформаційні потоки в обліковій політиці

підприємства. Якщо комунікації відбуваються напряму з контрагентом, необхідно з кожним суб'єктом господарювання (інституцією) укладати договір щодо схеми організації інформаційний зв'язків. Загальні умови договорів синхронізуються з обліковою політикою підприємства щодо порядку, технології та програмно-технічного забезпечення інформаційного обміну. Комунікаційні зв'язки з зовнішніми користувачами через використання посередника-оператора потребують підключення підприємства до загальних телекомунікаційних каналів зв'язку. Керівництву підприємства необхідно вибрати та відобразити в обліковій політиці методику комунікацій.

Як зазначають Боримська К.П. та Кінзерська Н.В., на ринку працюють спецоператори, які пропонують комплекс послуг з міжкорпоративного обміну електронною інформацією: 1) послуги з організації перманентного обміну даними – «підключення до мережі»; 2) послуги з передачі облікової інформації (після підключення) – «послуги зв'язку» [5, с.19]. Відмінною рисою методів зовнішніх комунікацій є кількість актів інформаційного обміну. При використанні методу комунікацій «підключення до мережі» обліковий відділ підприємства одержує облікову інформацію одразу після її надсилання від відправника. У іншому випадку («послуги зв'язку») в обліковій політиці рекомендовано зазначити час підключення програмного забезпечення до комунікаційних каналів з метою завантаження/вивантаження облікової інформації, акумульованої від моменту попереднього інформаційного обміну.

Загрозливим для інформаційної безпеки в автоматизованій системі обліку може бути шахрайське видозмінення спеціалізованого програмного забезпечення. В комп'ютерні програми можуть бути внесені зміни або вони можуть бути підмінені зловмисниками з метою викрадення конфіденційної облікової інформації. Інформаційний захист на підприємстві передбачає постійний контроль за автентичністю програмного забезпечення через механізм отримання та контролю електронних сертифікатів від розробників. З виробниками програмного забезпечення доцільно укласти договір про періодичне підтвердження

сертифікату достовірності. В обліковій політиці необхідно зазначити періодичність перевірки кожної комп'ютерної програми на предмет її автентичності та цілісності. Обов'язковим є підтвердження електронного сертифіката розробником після кожного поновлення програми.

Програмне забезпечення для цілей автоматизації обліку обов'язково повинно бути наділене наступними властивостями: сумісності з іншими комп'ютерними програмами, оперативного коригування помилок та внесення поправок без призупинення облікового процесу, відновлення результатів роботи у випадку пошкодження програмно-технічного забезпечення. Особливої уваги з позиції захисту облікової інформації потребує можливість інформаційної синхронізації програмних продуктів різних виробників. З метою організації вільного інформаційного обміну необхідно вказати в обліковій політиці тип протоколу чи формат обмінного файлу, який буде використаний для синхронізації. Визначення виду комунікаційних каналів при встановленні зв'язку між програмним забезпеченням дозволить мінімізувати інформаційні загрози втрати інформації чи її викрадення через використання невідомих протоколів обміну. Облікова політика регламентує порядок синхронного використання комп'ютерних програм, що не дасть змоги помилитися обліковим та управлінським фахівцям у процесі виконання функціональних обов'язків.

Аналогічно необхідно і визначити методику та відповідальних осіб за внесення правок у алгоритм роботи програмного забезпечення. Обліковим фахівцям з високим рівнем довіри до комерційної таємниці підприємства доцільно надати право коригування помилок та актуалізації комп'ютерних програм відповідно до змін національного законодавства чи інших чинників зовнішнього середовища. Також необхідно в обліковій політиці підприємства визначити порядок перманентного тестування програмних продуктів на предмет їх актуальності та коректності. В певні проміжки часу обліковим та управлінським фахівцям необхідно доручити можливість внесення та обробки змодельованої облікової інформації, яка має імовірнісний характер. Іншими словами, моделюється економічна ситуація у процесі функціонування підприємства з відповідним

відображенням в системі обліку та управління. Після підтвердження ефективності автоматизованих дій інформація вилучається із системи з метою уникнення впливу на реальні економічні показники діяльності суб'єкта господарювання. Залишається лише звіт, який передається для ознайомлення керівництву підприємства.

3.2. Вплив організаційних чинників та форм облікового аутсорсингу на кібербезпеку підприємств

Трансформація соціально-економічних процесів в умовах становлення цифрової економіки формує унікальні можливості для організації бухгалтерського обліку. Важливим оптимізаційним методом організації облікових процесів є їхнє делегування стороннім інституціям (аутсорсинг). Обліковий аутсорсинг в умовах використання комп'ютерно-комунікаційних технологій урізноманітнюється до декількох організаційних форм. Серед найбільш популярних форм організації делегування облікових повноважень слід виокремлювати аутсорсинг: спеціалізованою фірмою, незалежним обліковим фахівцем, імплементованим бухгалтером-аутстафером, хмарним сервісом обробки інформації.

Донедавна найбільш популярною формою облікового аутсорсингу було залучення спеціалізованої аутсорсингової фірми, штатні працівники якої виконують функції з обробки первинних даних та формування звітності підприємства. Досить часто делегування облікових повноважень реалізують аудиторські фірми, що є супутніми послугами аудиту. З дистанціюванням праці персоналу, зумовленого пандемією COVID-19 та військовими загрозами, актуалізується можливість передачі функцій обліку незалежним обліковим фахівцям. Такі зовнішні бухгалтери є самозайнятими особами і на основі договору надають послуги аутсорсингу.

Гібридною формою аутсорсингу, яка поєднує попередні варіанти, є аутстафінг. За умовами договору аутстафінгу облікові фахівці, що є штатними працівниками незалежної інституції імплементуються у функціональну структуру адміністративного персоналу підприємства. Аутстафери хоча і працюють на підприємстві, яке замовило послуги облікового аутсорсингу, але підпорядковані аутсорсинговій фірмі. Відповідальність за реалізацію облікових процесів несе фірма, що надає послуги аутстафінгу. Також розвиток комп'ютерно-комунікаційних технологій призвів до активізації хмарного делегування облікових повноважень. Хмарні сервіси аутсорсингу виконують найбільш трудомісткі типові процедури обробки інформації. Враховуючи значний рівень автоматизації обчислювальних робіт, хмарний аутсорсинг є більш оптимальним варіантом у частині організаційних витрат у порівнянні з іншими формами делегування облікових повноважень.

Разом з вартісним критерієм селекції організаційних форм аутсорсингу доцільно виокремлювати комплекс організаційних чинників, які характеризують методику та організацію обліку на підприємстві. Варіативність організаційних чинників є причиною вибору певної форми аутсорсингу для кожного суб'єкта господарювання, що мінімізує кіберризики його функціонування. Іншими словами, обраний організаційний варіант делегування облікових повноважень має забезпечувати максимальний рівень кіберзахисту підприємства.

Необхідності кіберзахисту підприємств в умовах аутсорсингу приділяється значна наукова увага. Зокрема, Nassimbeni G., Sartor M. та Dus D. дослідили причини та наслідки ризиків впровадження аутсорсингу та офшорінгу. Оцінюючи потенційні ризики за методом аналізу відмов і їхніх наслідків, науковці обґрунтували, що зростаючими загрозами реалізації аутсорсингу та офшорінгу є кіберзагрози функціонуванню підприємств [134]. Найбільш активні кіберзагрози, як доводить Benaroch M., актуальні для IT-аутсорсингу, що пояснюється вразливістю інформаційної системи підприємства при перманентному обміні інформацією з аутсорсером [59]. Almutairi M. і Riddle S. запропонували класифікацію кіберризиків IT-аутсорсингу для забезпечення кіберзахисту

підприємств. На основі удосконаленої класифікації науковцями розроблено методику управління ризиками у проектах аутсорсингу [51]. Продовжив дослідження ризик менеджменту у контексті кіберзахисту аутсорсингових комунікацій Cremonini M., який приділив увагу хмарним сервісам делегування інформаційно-функціональних повноважень [67]. На розмежування кіберризиків в умовах хмарного та нехмарного аутсорсингу наголошують Asatiani A. та інші. Науковці звертають увагу на різних організаційних чинниках, що впливають на кіберзахист в умовах делегування обробки облікової інформації [53]. З метою забезпечення окреслених проблем в кібербезпеці аутсорсингу Abdelwahab I., Ramadan N. і Hefny H. запропонували концепцію мінімізації кіберризиків на основі використання технології блокчейн [46].

Делегування облікових повноважень у більшості випадків призводить до зростання інформаційних загроз функціонуванню суб'єктів господарювання. Менеджмент підприємства зважає на очікувану користь від аутсорсингу, що компенсує потенційні кіберризики. Необхідність забезпечення кіберзахисту також враховується при оцінці економічної ефективності аутсорсингу. При втраті облікової інформації, що містить комерційну таємницю про певні економічні об'єкти чи явища, можливо визначити економічні витрати підприємства. Унаслідок прояву кіберзагроз можливе призупинення господарської діяльності, позиційні втрати клієнтів та ринку, недотримання термінів погашення кредиторської заборгованості і т.д., на що також доцільно зважати при розрахунку витрат на реалізацію аутсорсингу.

Отже, лише за прийнятного рівня кіберзагроз можливий аутсорсинг облікових повноважень. Кіберзагрози варіативно проявляються залежно від організаційної форми аутсорсингу, що полягає в делегуванні облікових повноважень: аутсорсинговій фірмі, сторонньому обліковому фахівцю, аутстаферу чи хмарному сервісу обробки інформації.

Найбільш важливим організаційним чинником, що вливає на кіберзахист підприємств, є облікова об'єктність – ступінь охоплення аутсорсингом облікових функцій. Інформація про облікові об'єкти, що передаються у компетенцію аутсорсеру, може бути конфіденційною

залежно від виду обліку. Делегування управлінського обліку, враховуючи його виняткове функціональне позиціонування для цілей внутрішніх користувачів інформації, може призвести до втрати комерційної таємниці. Натомість аутсорсинг фінансового обліку супроводжується мінімальними кіберризиками. Інформація фінансового обліку доступна для зовнішніх стейкхолдерів, а тому не потребує додаткового кіберзахисту. Отже, від кількості функціональних повноважень облікових фахівців, що делегуються аутсорсеру, безпосередньо залежить ймовірність прояву кіберзагроз.

Аналогічно й кількість працівників бухгалтерії визначає ризикованість аутсорсингу. Якщо у штаті підприємства лише один обліковий фахівець, делегування облікових повноважень є неможливим. Із збільшенням кількості облікового персоналу уможливлюється аутсорсинг обліку, що передбачає передачу частини повноважень третім особам. Організація облікового аутсорсингу сприяє оптимізації організаційної структури підприємства. На аутсорсинг передаються повноваження облікових працівників, функціонування яких не пов’язане з оперуванням комерційною таємницею підприємства. Штатні працівники можуть здійснювати інформаційну координацію між аутсорсером та обліковим підрозділом підприємства.

З функціонуванням облікових працівників також пов'язаний чинник невизначеності, що пояснюється невпевненістю менеджменту підприємства у ефективно функціонуючій системі обліку на підприємстві. Недостатній рівень знань та професійних навичок облікового персоналу загрожує діяльності суб’єкта господарювання. Першочергово зростає ймовірність появи кіберзагроз із зростанням невизначеності, пов’язаної з фаховістю облікових працівників. Тому делегування облікових повноважень працівників, щодо яких існує невизначеність, розглядається як спосіб забезпечення кіберзахисту підприємства. Аналогічно делегуванню підлягає облік об’єктів з критичним рівнем невизначеності, що може призвести до фінансових та інформаційних втрат.

Дистанційне виконання обліковими фахівцями функціональних повноважень визначає ризикованість аутсорсингу, що пояснюється

оптимізацією та захистом комунікаційних процесів на підприємстві. У суб'єктів господарювання, які практикують виконання посадових обов'язків з дому, обмін обліковою інформацією уже налагоджений. Відповідно, обліковий аутсорсинг може відбуватися з використанням уже налагоджених комунікаційних каналів, що не призводить до появи нових кіберризиків.

Необхідність реалізації ділових комунікацій з аутсорсером також є організаційним чинником, на який необхідно зважати при оцінці кіберризиків в умовах аутсорсингу. Якщо облікові працівники підприємства часто здійснюють професійне консультування, обмінюються обліковою інформацією, обновлюють програмне забезпечення в аутсорсера тощо, зростає ймовірність появи кіберризиків у процесі електронного комунікування. Нечасті або відсутні комунікації з аутсорсером унеможливлюють появу значних загроз кібербезпеці підприємства. Аналогічно обґрунтовується також необхідність налагодження комунікацій з контрагентами в умовах делегування облікових повноважень третім особам. Доступ аутсорсерів до конфіденційної інформації про покупців, постачальників, кредиторів тощо загрожує фінансово-господарській діяльності підприємства. Уможливлюється втрата ринків збуту, невиконання договорів постачання, ускладнення логістичних ланцюгів поставок, погіршення ліквідності та платоспроможності підприємства, що зумовлені проявом фінансових та інформаційних загроз.

На кібербезпеку підприємства також впливає рівень автоматизації облікових робіт. З однієї сторони комплексна автоматизація облікових функцій передбачає цифровізацію усіх бізнес-процесів, що призводить до зростання імовірності прояву кіберзагроз втрати великих масивів конфіденційної інформації при аутсорсингу. З іншої – реалізація облікових функцій без використання комп'ютерно-комунікаційних технологій є ускладненою в умовах аутсорсингу. Делегування неавтоматизованих операцій обробки облікової інформації також призводить до виникнення загроз кібербезпеки підприємств унаслідок необхідності оптимізації аутсорсером усіх бізнес-процесів. В такому

випадку аутсорсер отримує повний доступ до комерційної таємниці, що максимізує кіберзагрози. Тому оптимальним варіантом облікового аутсорсингу є делегування облікових повноважень з частковою автоматизацією.

Також на кібербезпеку підприємств в умовах облікового аутсорсингу має вплив частота інформаційних актів в обліковому процесі. Якщо обробка облікової інформації відбувається перманентно, їхнє делегування третім особам призводить до потенційного порушення безпекового режиму. На підприємствах з незначною інтенсивністю фінансово-господарських подій та, відповідно, кількістю інформаційних актів (декілька в день або декілька в тиждень) обліковий аутсорсинг не значно впливає на кібербезпеку. Перманентні облікові процеси, як правило, залишаються у компетенції облікового підрозділу підприємства. Натомість, періодичні інформаційні акти частіше делегуються аутсорсерам без значних кіберризиків.

Зважаючи на організаційні чинники, менеджмент підприємства приймає рішення про імплементацію такої форми облікового аутсорсингу, яка мінімізує ймовірність прояву кіберризиків. Для оцінки рівня кіберзахисту за варіативними організаційними чинниками та формами аутсорсингу доцільно використати аналіз, наведений в табл. 3.1.

Залежно від внутрішніх та зовнішніх умов функціонування суб'єктів господарювання, що визначає їхню облікову політику, змінюються організаційні чинники обліку. У табл. 1 виявлено вплив організаційних чинників (№ 1-8) на імовірність прояву кіберризиків для кожної форми аутсорсингу за варіантами (1 – спеціалізована аутсорсингова фірма, 2 – незалежний обліковий фахівець, 3 – імплементований бухгалтер аутстафер, 4 – хмарний сервіс обробки інформації). Кожний організаційний чинник диференційовано впливає на кіберзахист підприємства для різних форм аутсорсингу. Наприклад, «об'єктність» обліку (чинник № 1) є причиною збільшення ймовірності прояву кіберризиків для варіантів 2 і 3, що пояснюється недостатньою відповідальністю індивідуальних облікових фахівців – суб'єктів аутсорсингу за зберігання конфіденційності інформації.

Таблиця 3.1

Оцінка ймовірності прояву кіберризиків у розрізі організаційних чинників обліку та форм облікового аутсорсингу

№ чинника	Організаційний чинник / характеристика обліку	Форма аутсорсингу			
		1 варіант	2 варіант	3 варіант	4 варіант
		Аутсорсингова фірма	Незалежний обліковий фахівець	Імплементований бухгалтер аудстафер	Хмарний сервіс
1.	- Об'єктність				
	фінансовий облік	0	0,1	0,2	0
	управлінський облік	0,7	1	1	0,5
2.	- Кількість працівників				
	1	0,9	0,9	1	0,7
	2-5	0,6	0,7	0,3	0,3
	>6	0,3	0,3	0	0,3
3.	- Невизначеність				
	високий рівень	0,2	0,8	0,8	0,2
	помірний рівень	0	0,5	0,5	0,3
	низький рівень	0	0,2	0,2	0,2
4.	- Дистанційність				
	відсутня	0,7	0,7	1	0,9
	присутня	0,2	0,2	0,9	0,1
5.	- Комунікації з аутсорсером				
	відсутні	0	0	0	0
	присутні	0,3	0,3	0,3	0,9
6.	- Комунікації з контрагентами				
	відсутні	0	0	0	0
	присутні	0,7	0,7	0,7	1
7.	- Автоматизація				
	відсутня	1	1	1	0,8
	часткова	0,2	0,2	0,2	0,2
	комплексна	0,6	0,6	0,6	0,2
8.	- Частота				
	перманентно	1	1	1	0,7
	декілька у день	0,7	0,7	0,7	0,3
	декілька у тиждень	0,2	0,2	0,2	0,2

Ймовірність прояву кіберризиків оцінюється за шкалою: 0 – відсутні кіберзагрози, 0,1-0,3 – кіберзагрози малоймовірні, 0,4-0,7 – кіберзагрози середньо ймовірні, 0,8-1 – кіберзагрози з високою ймовірністю.

Джерело: розроблено автором

При врахуванні кількості облікових фахівців (чинник № 2) у процесі аутсорсингу найменша імовірність прояву кіберризиків у варіанті 3. Штатні облікові фахівці можуть здійснювати контроль за функціонуванням аутстафера. Також функціональними обов'язками імплементованих бухгалтерів можуть бути об'єкти обліку, які не пов'язані з комерційною таємницею підприємства.

«Невизначеність» в обліку (чинник № 3) та пов'язані кіберризики повністю нівелюється при делегуванні облікових повноважень аутсорсинговій фірмі унаслідок залучення штату висококваліфікованих фахівців у різних сферах. Натомість, використання послуг одного незалежного або імплементованого бухгалтера (варіанти 2 і 3) позитивно не впливає на кібербезпеку підприємства, оскільки також існують сумніви щодо кваліфікації таких облікових фахівців.

Дистанційність у виконанні облікових повноважень (чинник № 4) мінімізує кіберризики для усіх форм аутсорсингу окрім делегування обліку імплементованому бухгалтеру-аутстаферу. Оскільки аутстафінг передбачає введення в структуру бухгалтерії підприємства працівника аутсорсера (варіант 3), дистанціювання його роботи не призводить до мінімізації кіберризиків. Аналогічно й необхідність комунікацій з аутсорсером (чинник № 5) в умовах використання послуг хмарної обробки облікової інформації (варіант 4) відрізняється від інших форм аутсорсингу. Оскільки хмарні сервіси не надають комплексних, мультиаспектних професійних консультацій унаслідок відсутності прямих комунікацій з обліковими фахівцями, значно зростають кіберризики. За повністю схожою методикою оцінюються кіберризики і для комунікацій з контрагентами (чинник № 6), що демонструє найнижчий рівень кіберзахисту для хмарного варіанту аутсорсингу.

Натомість, ступінь автоматизації облікових робіт (чинник № 7) та «частота» обліку (чинник № 8) майже не впливає на кібербезпеку підприємств за різних форм аутсорсингу, оскільки незалежно від організаційного варіанту присутні рівномірні кіберризики.

Найбільш оптимальною формою аутсорсингу для суб'єкта господарювання є варіант з мінімальною сумарною імовірністю прояву

кіберризиків за усіма організаційними чинниками обліку. Кіберризики значно мінімізуються при делегуванні облікових повноважень хмарним сервісам (варіант 4), функціональними обмеженнями якого є ускладненість перманентних комунікацій аутсорсера з менеджментом підприємства та контрагентами, що не дає змоги рекомендувати таку форму аутсорсингу для усіх суб'єктів господарювання. Тому, додаткового врахування та подальшого дослідження потребує вплив організаційно-правової форми, економічної галузі, розміру бізнесу, кількості працівників на кібербезпеку підприємства в умовах облікового аутсорсингу.

3.3. Комбінований (інтегрований) аутсорсинг облікових та кібербезпекових повноважень

Облікова діяльність сучасних підприємств ускладнюється через численні організаційні обмеження. Перманентні зміни законодавства у сфері обліку і оподаткування передбачають адекватну адаптацію облікової практики. Несвоєчасне врахування вимог нормативно-правових документів може призвести до штрафів та інших фінансових санкцій. До облікових фахівців ставляться вимоги мультикваліфікованості та періодичного перенавчання відповідно до змін соціально-економічних чи юридичних чинників. Оновлення знань та вмінь персоналу підприємства потребує залучення значних інформаційних і фінансових ресурсів. На час удосконалення облікової політики та актуалізації навичок персоналу у зв'язку з відсутністю на робочому місці (неможливості дистанційно виконувати функціональні повноваження) зростає імовірність призупинення діяльності суб'єктів господарювання, що призведе до недоотримання операційних доходів.

Для попередження непродуктивних простоїв у діяльності менеджмент підприємства досить часто збільшує штат облікових працівників. Зростання штатного персоналу неодмінно призводить до актуалізації кіберзагроз для суб'єктів господарювання. Ефективним методом

забезпечення кібербезпеки є обмеження доступу облікових фахівців до певних масивів даних. Позиція менеджменту підприємства полягає у необхідності розподілу функціональних обов'язків працівників за різними об'єктами обліку з одночасним дозуванням облікової інформації. Додатково діяльність кожного облікового фахівця контролюється відділом кіберзахисту. Таким чином, менеджмент, бажаючи мінімізувати фінансові та інформаційні втрати, водночас збільшує адміністративні витрати на утримання надмірно великого штату підприємства.

Актуалізується питання про оптимізацію витрат на дуальну організацію обліково-безпекових функцій. Підприємства великого бізнес-розміру досить часто вдаються до послуг аутсорсингу, що передбачає делегування повноважень з реалізації обліку та кібербезпеки третім особам.

Серед недоліків аутсорсингу обліку Назаренко О. В., Суровицька А. В. виокремлюють: виникнення витрат, пов'язаних із передачею функцій на аутсорсинг; необхідність співпраці лише з одним аутсорсером; загроза рейдерської атаки з боку аутсорсера; ризик потрапляння комерційної інформації до конкурента [26]. Доповнюють перелік загроз реалізації облікового аутсорсингу Лобода Н. О., Чабанюк О. М., Сенишин Б. Б., серед яких виокремлено: недоступність облікової бази даних, конфіденційність інформації, витік інформації, втрата оперативності, відсутність управлінського обліку [20]. На аналогічних загрозах аутсорсингу звертає увагу також й Maszczak T., але з врахуванням розміру та організаційно-правової форми суб'єктів господарювання, кількості працівників, прибутковості бізнесу тощо [122]. Проте, науковцями не враховано, що більшість організаційних обмежень усуваються незалежно від виду суб'єктів господарювання за допомогою застосування комп'ютерно-комунікаційних технологій в обліку та функціональної інтеграції теорії аутсорсингу з іншими науковими концепціями й предметними дослідженнями.

Зокрема, різними науковцями досліджено інтегруючі особливості обліку у контексті його делегування: Martyniuk T. – функціонально-інформаційну єдність обліку та фінансів в умовах їхнього аутсорсингу, що

позиціонує технічні вимоги до організації автоматизованої обробки облікової інформації [121]; Alkarawy H. й AL-Kuwair E. – взаємозв'язок між обліковим аутсорсингом та менеджментом, що сприяє реінжинірингу усіх бізнес-процесів підприємства [49]; Nicholson B. та Aman A. – обліковий механізм формування офшорних зон, які ґрунтуються на делегуванні обліку та фінансів третім особам [136]; Cullinan C. та Zheng X. – взаємовплив аутсорсингу обліку та аудиту, що зменшує потребу в аудиторському контролі унаслідок оптимізації інформаційної координації між учасниками управлінського процесу на підприємстві [68]; Sofiah Aman A., Maelah R., Amiruddin R. та Hamzah N. – необхідність фінансового контролю за процесом аутсорсингу облікових функцій для обґрунтування його доцільності та ефективності [171] тощо.

Для аналізу ефективності аутсорсингу на етапі пост-імплементації проекту з делегування облікових функцій Samudrage D. і Jayewardene D. розроблена система збалансованих показників. Дослідження на прикладі підприємств різних видів діяльності продемонструвало ефективність та виправданість інвестування в обліковий аутсорсинг [155]. Але при розрахунку запропонованих показників не були враховані потенційні втрати та вигоди від захисту інформації. З іншого боку, присутні наукові дослідження безпекових аспектів аутсорсингу обробки економічної інформації третім особам (Liu Z. та інші [117]; Stitilis D. та інші [174]) або хмарним сервісам з наданням різностороннього доступу до баз облікових даних (Asatiani A. [53]), які не враховують облікової природи інформаційних процесів в економіці.

У той же час, як доводять дослідження «The 2019 Kearney Global Services Location Index», серед досліджених підприємств найбільш популярними напрямками аутсорсингу є IT-послуги (40,5 %), логістика (35,2 %) та бухгалтерський облік (32,4 %, з яких: загальні функції обліку – 13,5 %, облік заробітної плати – 13,5 %, кадровий облік – 5,4 %) [72] (рис. 3.2).

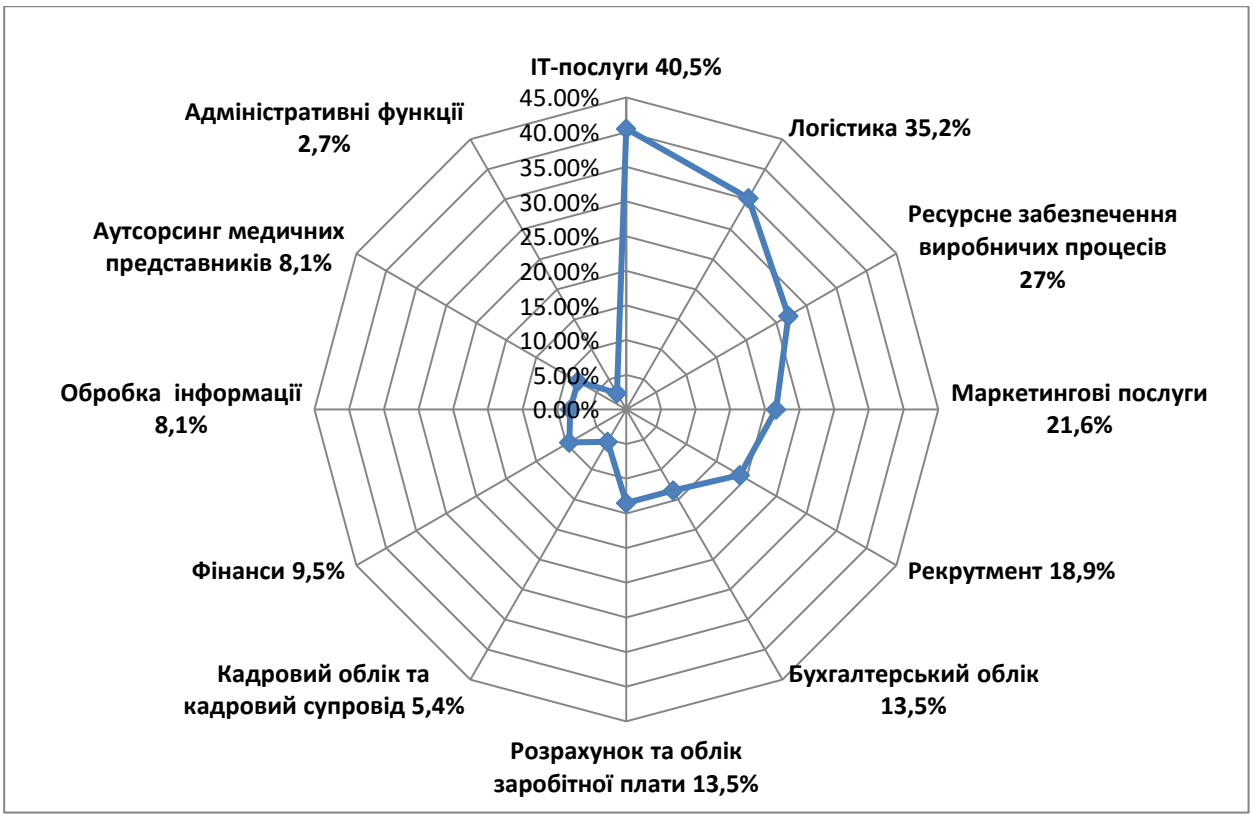


Рис. 3.2. Популярність аутсорсингу у розрізі делегованих бізнес функцій

Джерело: [72; 200]

Деякі з опитаних підприємств здійснювали одночасно аутсорсинг за декількома напрямами. Інтеграція найбільш популярних напрямків аутсорсингу (IT-послуг та бухгалтерського обліку) забезпечує синергетичну оптимізацію бізнес-процесів, які делеговані, та мінімізацію витрат підприємства. Паралельний аутсорсинг облікових та безпекових функцій сприяє мінімізації інформаційних та фінансових ризиків підприємств. Тому, якщо реалізація облікових функцій у значній мірі автоматизована та передається третім особам, доцільно делегувати також забезпечення кіберзахисту підприємств. Проте уточнення потребує організація інтегрованого аутсорсингу обліково-безпекових повноважень з врахуванням: конфіденційності облікових даних, необхідності регламентації прав доступу до комерційної таємниці, автоматизації обробки і передачі інформації з використанням сучасних комп'ютерно-комунікаційних технологій.

В бухгалтерському обліку інформація поділяється на вільнодоступну та конфіденційну. Дані фінансового обліку публічно оприлюднюються і за вимогою передаються усім зацікавленим особам, а тому не потребують додаткового кіберзахисту. Функції фінансового обліку можна повністю делегувати третім особам. Натомість, дані управлінського обліку містять комерційну таємницю і піддаються активним кіберзагрозам. Конфіденційна інформація не повинна покидати інформаційні межі підприємства, що утруднює аутсорсинг управлінського обліку. Кіберзахист такої інформації потребує залучення кібербезпекових фахівців та ресурсів на макрорівні підприємства.

Для інтегрованого аутсорсингу облікових та кібербезпекових повноважень доцільно використовувати такі організаційні моделі: об'єктна, структурна, комбінована (мозаїчна). Основним відмінним критерієм виокремлення організаційних моделей аутсорсингу є ступінь охоплення обліково-безпекових функцій, що підлягають делегуванню у розрізі облікових об'єктів та видів обліку або структурних підрозділів підприємства.

Відповідно до першого варіанту аутсорсингу делегуванню повністю підлягає фінансовий облік. Контроль та кіберзахист даних фінансового обліку, що не містить комерційної таємниці, доцільно також передати третім особам. Проте реалізацією управлінського обліку і його кіберзахисту повинен займатися власний обліково-безпековий підрозділ підприємства. Після збору первинні дані доцільно автоматизовано розподіляти між бухгалтерією для цілей управлінського обліку та консалтинговою фірмою в дозованій формі – фінансового обліку.

Об'єктне поле фінансового обліку додатково можливо поділити на підмножини. Делегуванню можуть підлягати найбільш трудомісткі аспекти фінансового обліку у розрізі окремих облікових об'єктів. Наприклад, облік заробітної плати чи розрахунків за податками і зборами доцільно передавати аутсорсеру для мінімізації втрати фінансових ресурсів на погашення можливих штрафних санкцій у зв'язку з некоректною реалізацією облікових методик чи порушення законодавства.

В такому випадку кібербезпекові функції також розподіляються пропорційно делегованим обліковим повноваженням.

При використанні першої об'єктної моделі мінімізуються кіберризики підприємства. Передача як і гіпотетична втрата даних фінансового обліку в умовах його делегування не загрожує кібербезпеці підприємства. Управлінський облік та його кіберзахист внутрішніми організаційними інституціями реалізується на рівні підприємства, що превентивно нейтралізує кіберзагрози.

За умовами другої організаційної моделі делегувати можливо функції фінансового і управлінського обліку та кіберзахисту у розрізі окремих структурних підрозділів підприємства. В організаційній структурі підприємства виокремлюють центри відповідальності, дочірні підприємства, територіально відокремлені підприємства, філії, відділи, що самостійно реалізують вимоги бухгалтерського обліку. Використання структурної організаційної моделі передбачає делегування комплексу обліково-безпекових повноважень аутсорсеру в інформаційних рамках відокремленої господарської одиниці. Бухгалтерія як організаційна одиниця може бути відсутня у територіально відокремлених підрозділах у в'язку з повним делегуванням фінансового та управлінського обліку третім особам. То такого виду аутсорсингу можуть вдаватися територіально-відокремлені підрозділи підприємства, які функціонують у правовому полі інших держав, що значно відрізняє методику обліку в материнській та дочірніх суб'єктах господарювання. Аутсорсер в такому випадку нівелює національні відмінності в організації обліку.

Для мінімізації кіберризиків консолідацію облікової інформації та її кіберзахист в умовах аутсорсингу доцільно здійснювати в обліково-безпековому підрозділі підприємства (материнської фірми, центрального офісу, адміністративного підрозділу. У випадку кібератак підприємству загрожує втрата лише епізодичної (частковою) облікової інформації про функціонування окремої господарської одиниці. Загальна цілісність інформаційної моделі функціонування суб'єкта господарювання не порушується унаслідок точкових кіберзагроз. Проте додаткові функції кіберзахисту покладаються на штатних працівників, які зобов'язані

забезпечити кібербезпеку при отриманні від відокремлених господарських одиниць облікової інформації та її акумулюванні в бухгалтерії підприємства. Інформаційну схему об'єктної та структурної організаційної моделі аутсорсингу відображено на рис. 3.3.

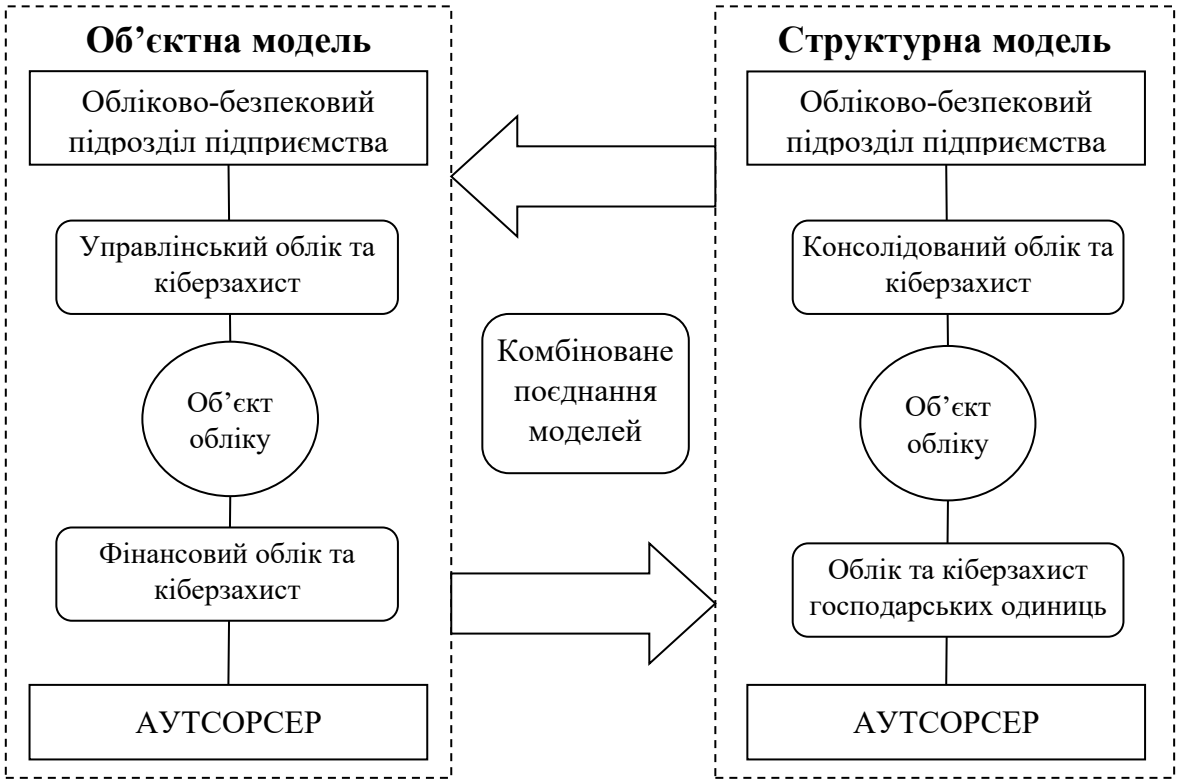


Рис. 3.3. Об'єктна та структурна організаційні моделі аутсорсингу
Джерело: розроблено авторами

Отже, об'єктна і структурна організаційні моделі аутсорсингу передбачають дуальну реалізацію облікових функцій паралельно бухгалтерією підприємства та третіми особами. Зростання обсягу делегованих повноважень з обробки облікових даних та їхнього кіберзахисту уможливлює втрату конфіденційної інформації та інформаційні шахрайства чи зловмисні маніпуляції. Тому комплексна передача обліково-безпекових повноважень аутсорсеру є ускладненим у зв'язку з проявом значних кіберризиків.

Для забезпечення ефективного кіберзахисту та уникнення організаційних обмежень реалізації об'єктного і структурного варіантів аутсорсингу доцільно використовувати комбіновану (мозаїчну) модель. Основна ідея запропонованої організаційної моделі полягає у поєднані

особливостей об’єктного та структурного варіантів аутсорсингу з мозаїчним делегуванням обліково-безпекових функцій багатьом аутсорсерам. Усі завдання обліку та кіберзахисту поділяються на декілька підмножин, які передаються різним третім особам.

Первинним елементом автоматизованого обліку може бути система технологічних датчиків, які функціонують на принципах технології Інтернету речей. Технологічними пристроями збору облікових даних, функціонуючих на принципах технології Інтернету речей, може бути обладнання для цілей: роботизованого виробництва, радіочастотної ідентифікації матеріальних цінностей, біометрії працівників, верифікації оплати за послуги, електронних грошових трансакцій, GPS-навігації транспорту тощо. Облікові дані, автоматизовано зібрані з використанням Інтернету речей, одразу надсилаються через глобальну мережу до місць їх обробки чи зберігання. Технологічні датчики працюють автономно без прямої участі облікових фахівців, що мінімізує фінансові та кіберризики. В облікових працівників відсутній повний доступ до інформації на етапі її збору, відповідно, унеможливлюються зловмисні інформаційні маніпуляції. Залишається необхідність у забезпеченні контролю за функціонуванням облікових та управлінських працівників на подальших етапах обробки інформації для цілей її кіберзахисту.

Зібрані з використанням технології Інтернету речей первинні дані підлягають кластеризації, накопиченню та передачі користувачам для подальшої обробки. Класифікована облікова інформація транслюється стейкхолдерам (в тому числі аутсорсерам) в обмеженому обсязі відповідно до прав доступу та функціональних обов’язків. Інформаційні комунікації відбуваються винятково в електронній формі на принципах дистанційності. Аутсорсери можуть перебувати на значній територіальній віддаленості від місць генерування первинних даних. Завдяки відсутності просторових обмежень кількість аутсорсерів, залучених до реалізації обліково-безпекових повноважень, може бути необмеженою. Додатково, частина функцій автоматичної обробки облікової інформації виконуються хмарними сервісами. Залучення значної кількості учасників до

інформаційного процесу потребує використання дієвих комунікаційних механізмів та мережевих технологій.

Фундаментальною основою комбінованого (мозаїчного) варіанту аутсорсингу доцільно обрати мережеву технологію блокчейн, яка поєднує облікові фрагменти в єдину інформаційну модель функціонування підприємства. Інформаційну схему комбінованої (мозаїчної) організаційної моделі аутсорсингу відображено на рис. 3.4.

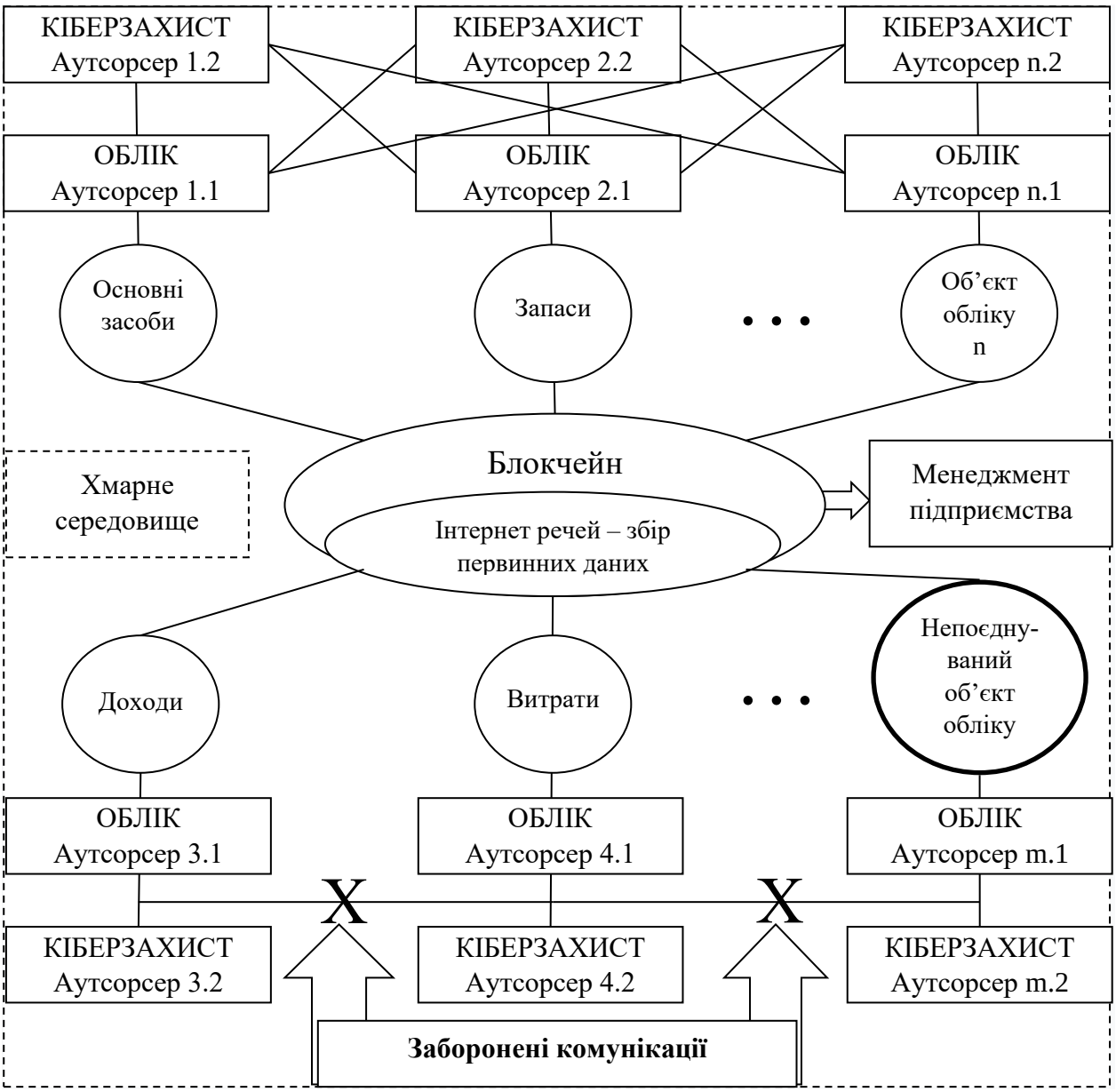


Рис. 3.4. Комбінована (мозаїчна) організаційна модель аутсорсингу

Джерело: розроблено авторами

Ведення фінансового та управлінського облік у розрізі їхніх об’єктів доцільно делегувати що раз іншій фірмі, яка надає послуги аутсорсингу. Також не рекомендується передавати функції з обліку та одночасно кіберзахисту даних за певним обліковим об’єктом одній аутсорсинговій фірмі. Наприклад, облік та кіберзахист інформації про витрати підприємства мають здійснювати різні аутсорсери. Розрізнене делегування обліково-безпекових функцій зменшує імовірність настання кіберзагроз та втрати критично великих масивів даних, що загрожує функціонуванню підприємств. Критично важливо розмежовувати облікову інформацію, що потрапляє до одного аутсорсера щодо певних об’єктів обліку. Наприклад, недоцільно одночасно делегувати повноваження з обліку доходів і витрат третій особі, що може призвести до втрати інформації про прибутки чи збитки підприємства.

Поділ інформаційного поля функціонування підприємства може здійснюватися на більш деталізовані множини. Різним аутсорсерам доцільно передавати на опрацювання облікову інформацію про певний об’єкт обліку ще й у розрізі різних часових періодів, господарських одиниць, працівників підприємства, виробничих процесів тощо. За допомогою технології блокчейн розрізнена облікова інформація інтегрується і передається бухгалтерії та менеджменту підприємства для подальшого опрацювання. Кожний аутсорсер оперує винятково мозаїчними масивами даних, необхідними для реалізації часткових облікових або безпекових функцій.

ВИСНОВКИ

1. Зростання активності кібератак як частина військово-гібридного впливу на соціально-економічні процеси та загроза втрати конфіденційної інформації визначили необхідність забезпечення кібербезпеки підприємств, секторів та галузей економіки. Враховуючи продукуючу природу бухгалтерського обліку як основного генератора економічної інформації, пріоритетного кіберзахисту потребує облікова система суб'єктів господарювання. Систему бухгалтерського обліку на підприємстві доцільно позиціонувати важливим елементом організації кібербезпеки у зв'язку з: конфіденційністю значної частини облікової інформації; мультикваліфікованістю сучасних облікових фахівців з різних галузей знань; активністю кібератак через бухгалтерське програмне забезпечення; регламентуючою природою внутрішніх нормативних документів щодо інформаційно-безпекових процесів.

Для організації кібербезпеки необхідною є трансформація облікового підрозділу та функціональних обов'язків облікових фахівців у напрямку забезпечення інформаційної безпеки підприємств. Облікових фахівців доцільно залучати до міждисциплінарних команд у контексті забезпечення ефективного кіберзахисту підприємств. Разом із організацією дієвої кібербезпеки на підприємстві реалізації потребує перманентний безпековий аудит. Здійснення контролю і тестування системи кібербезпеки може виконуватися внутрішніми контролерами (обліковими фахівцями) або зовнішніми аудиторами, що формує новий масштабний ринок аудиторських послуг безпекового характеру.

2. Для уніфікації засобів забезпечення кібербезпеки підприємств необхідною є орієнтація на єдині фундаментальні принципи кіберзахисту облікової інформації. Основним принципом у забезпечені цінності облікової інформації є її надійність. Надійність облікової інформації засвідчує відсутність помилок, викривлень, неточностей, спричинених сторонніми особами, а також гарантує доступність та конфіденційність. Надійність інформації формується на перетині предметних областей

принципів бухгалтерського обліку та принципів інформатики. Отримання надійної облікової інформації є кінцевою метою комбінованого функціонування облікової та безпекової систем.

З надійністю облікових даних пов’язані принципи конфіденційності, цілісності і доступності. Дотримання безпекових принципів гарантує потрапляння якісної облікової інформації до внутрішніх та зовнішніх стейкхолдерів без втрати комерційної таємниці підприємства. Доповнюють теоретичний фундамент кіберзахисту облікової інформації принципи повноти, санкціонованості, адресності, достовірності і порівнюваності. Наведені принципи є фундаментом вироблення методичних інструкцій з кіберзахисту підприємств для попередження, уникнення та усунення наслідків загроз безпеці облікової інформації.

3. Необхідність організації ефективного кіберзахисту облікової інформації передбачає адаптивне врахування варіативних кіберзагроз. Залежно від виду кіберризиків можуть значно відрізнятися заходи їхнього попередження, уникнення та усунення потенційних наслідків. Тому кіберризики облікової інформації доцільно поділяти за класифікаційними критеріями: випадковості, цілеспрямованості, інформаційного та фінансового інтересу, територіальності, джерела виникнення, походження, об’єктності, предметності, масштабності, форми реалізації, кримінальності, аспектності, пролонгованості, латентності, ймовірності, наслідків. Класифікація за іншими критеріальними ознаками, що стосується діяльності зловмисників чи стейкхолдерів, є малоінформативною для цілей захисту від кіберзагроз.

4. Кінцевою метою реалізації кіберзагроз є отримання економічної вигоди третіми особами або завдання економічної шкоди суб’єктам господарювання. Існує пряма залежність між кіберризиками та економічним станом підприємства. Бухгалтерський облік доцільно позиціонувати як інноваційний механізм забезпечення взаємозв’язку між економічною та кібербезпекою підприємства. Обліковий зв'язок реалізується на п’яти рівнях, які адитивно наростають, і пояснює вплив активності кіберризиків на зростання загроз економічній безпеці суб’єктів господарювання. На методологічному рівні можливо обґрунтувати

кіберзагрози принципам та функціям обліку; на якісному рівні – якості облікової інформації; на методичному рівні – обліковим об’єктам та видам обліку; на комунікаційному рівні – обліковим комунікаціям зі стейкхолдерами; на репутаційному рівні – діловому іміджу підприємства, що призводить до економічних втрат підприємств. Водночас за допомогою методики бухгалтерського обліку реалізується зворотній інформаційний зв'язок економічної та кібербезпеки, що полягає в достовірній ідентифікації та оцінці економічних втрат від прояву кіберризиків.

5. Кіберзагрози проявляються на усіх етапах обробки облікової інформації та її передачі до користувачів (стейкхолдерів). Для вироблення дієвих заходів мінімізації кіберзагроз необхідне розуміння їхнього впливу на функціонування стейкхолдерів у розрізі різних їхніх видів. Традиційна класифікація користувачів облікової інформації є неактуальною для цілей забезпечення кібербезпеки підприємств, оскільки не враховує активізацію варіативних кіберзагроз, що потребує удосконалення класифікації стейкхолдерів. Користувачів облікової інформації доцільно класифікувати за критеріями: можливості управляти діяльністю господарюючого суб’єкта, правом доступу, імовірності появи кіберзагроз, можливості розпоряджатися правом доступу, доступу до облікових об’єктів, функціонального права, порядку обробки інформації, виду економічної діяльності, віку фізичних осіб, організаційно-правової форми юридичних осіб, виду застосовуваних комунікаційних каналів, частоти інформаційних актів. Використання запропонованої класифікації стейкхолдерів сприяє виявленню кіберризиків; попередженню, уникненню та мінімізації наслідків кіберзагроз, актуальних окремо для кожного виду користувачів облікової інформації.

6. Первинним методичним прийомом бухгалтерського обліку, на який слід звертати увагу при організації кіберзахисту, є документування явищ і подій. Традиційний електронний документообіг в бухгалтерському обліку має ряд функціональних обмежень, що є причиною вразливостей кібербезпеки підприємств. Для реалізації ефективних внутрішніх та зовнішніх електронних комунікацій доцільною є імплементація технології

блокчейн у документообіг, яка відповідає сучасним вимогам кіберзахисту підприємств. Факт збору первинних даних ініціює старт подальших інформаційних процесів обробки та розподілу облікової інформації. Задокументовані дані з використанням технології блокчейн фрагментуються, шифруються та надсилаються у дозованій формі внутрішнім та зовнішнім користувачам відповідно до інформаційних потреб та прав доступу до комерційної таємниці. Дозвільний режим обробки облікової інформації доцільно реалізувати з використанням системи цифрових підписів та хмарного розміщення розподілених баз даних.

Застосування технології блокчейн в електронному документуванні й документообігу забезпечує: фрагментованість, взаємне доповнення, масштабованість, дублювання, хронологічність, конфіденційність, розподіленість, доступність, відкритість обробки облікової інформації, що є основою в забезпеченні ефективного кіберзахисту підприємства. Організація кібербезпеки в умовах розподіленого структурування облікової інформації сприяє відкритості документообігу на підприємстві, що зменшує необхідність у застосуванні ізоляційних інформаційних практик. Відкритість інформаційного обміну з використанням технології блокчейн для кіберзахисту інформації мінімізує організаційні обмеження у становленні цифрової економіки та створює сприятливі умови для поступального інноваційного розвитку суспільної формації.

7. Основним об’єктом кібератак є грошові кошти підприємств. Необхідність отримання оперативного доступу до грошових коштів через електронні комунікації, захисту інвестицій після глобальних фінансових криз призвела до появи нового виду електронних грошей – криптовалют, які характеризуються такими перевагами, як: зручність, незалежність, доступність, дистанційність, конфіденційність, бездокументність, повна автоматизація обліку та оптимізація витрат.

Сучасні системи дистанційного управління рахунками «Клієнт-банк» та «Інтернет-банк» характеризуються певними організаційними обмеженнями, що не відповідають вимогам кібербезпеки. Об’єднання функціональних можливостей технології блокчейн, позитивних якостей

комунікацій «Інтернет-банк» та «Клієнт-банк» дозволить створити гібридну безпечну систему безготівкових платежів криптовалютами, електронними грошима, коштами на рахунках в банку з вільною конвертацією існуючих грошових засобів та можливостей інформаційного обміну з усіма учасниками розрахункових операцій.

Збір облікової інформації про розрахунки криптовалютами та іншими електронними грошима відбувається без формування традиційних платіжних документів та банківських виписок, що запобігає втраті конфіденційної облікової інформації. Електронна інформація з гібридної системи комунікацій є основою для автоматизованого документування, формування облікових записів, інформування фахівців з обліку та управління щодо безготівкових переказів. Автоматизація обліку грошових трансакцій сприяє забезпеченню ефективного кіберзахисту за виконанням грошових трансакцій та своєчасному і дистанційному інформуванню персоналу підприємства про параметри безготівкових платежів.

8. Важливим напрямом забезпечення кібербезпеки облікової інформації є використання технології Інтернету речей (IoT). Застосування IoT технології в автоматизації обліку та кіберзахисті підприємства можливе у трьох напрямках: трансформації бухгалтерського обліку, удосконаленні аудиторського контролю господарської діяльності та оптимізації роботи обліково-контролюючих фахівців. Застосування IoT-пристроїв забезпечує: зменшення участі людського чинника в обробці облікової інформації, дистанціювання збору та обробки первинних даних, автоматизацію документування господарських операцій, делегування обліково-контрольних та безпекових повноважень, дотримання якісних характеристик інформації та удосконалення форми бухгалтерського обліку для оперування значними масиви даних.

Поряд зі значними перевагами імплементації IoT-технології у діяльність підприємств виникають активні кіберризики. Загрозами кібербезпеці суб’єктів господарювання є викрадення, підміна та блокування інформації, а також отримання контролю над обладнанням або відмова його функціонування, підвищення прав доступу працівників і сторонніх осіб для проникнення у заборонені територіально-інформаційні

межі підприємства. Для уникнення та подолання наслідків кіберзагроз при використанні IoT-пристроїв необхідним є регламентація комунікаційних каналів передачі облікової інформації, регламентація прав доступу до конфіденційних даних, використання політики перманентного оновлення паролів для доступу до баз даних й технологічних датчиків, коректний розподіл інформаційних потоків між різними стейкхолдерами. Тому ризики імплементації технології IoT значно мінімізуються за умови ефективної організації бухгалтерського обліку з його позиціонуванням як базису налагодження кіберзахисту інформаційних потоків.

9. Для забезпечення контролю за доступом працівників до інформаційно-матеріальних потоків використовуються автоматизовані системи пропуску працівників на територію та приміщення підприємства. Експлуатація системи в основному передбачає реалізацію охоронних функцій. Проте, в умовах зростання кібернетичних загроз унаслідок міжнародних військово-гібридних конфліктів та біологічних загроз через пандемію COVID-19 зростає необхідність запровадження технології біометричної ідентифікації працівників, що передбачає трансформацію обліку і контролю відпрацьованого часу персоналом, нарахованої основної та додаткової заробітної плати, а також формування в електронній формі первинних та звітних документів з відправкою стейкхолдерам.

Біометричну ідентифікацію персоналу доцільно задіювати в місцях перетину працівниками просторових меж підприємства та окремих його приміщень. Усю територію суб'єкта господарювання необхідно розділити на різні функціональні зони для різних груп персоналу з метою обмеження доступу до конфіденційної інформації, що сприятиме забезпеченню належного рівня кіберзахисту підприємства. Нарахування заробітної плати рекомендовано здійснювати, виходячи з часу, проведеного у приміщеннях функціонального призначення персоналу або за обладнанням при виконанні посадових повноважень (у тому числі з дому). Для автоматизованого обліку і контролю попередньо розробляються функціонально-часові регламенти реалізації функціональних обов'язків та перебування у певних видах приміщення підприємства для кожного

працівника. Регламентування часових параметрів роботи працівників сприяє уникненню надмірного скупчення працівників у приміщеннях підприємства, що сприятиме мінімізації біологічних загроз (інфікування COVID-19).

Для ефективного обліку і контролю відпрацьованого часу доцільно впровадити калькуляційну одиницю – хвилина (хвилино-людина). Із застосуванням деталізованої одиниці часу з'являється можливість обліку і контролю відхилень від нормативів робочого часу, забезпечення самоконтролю працівників, зростання продуктивності їх праці. Недотримання часового режиму праці може бути підставою для перегляду умов праці чи потреби у професійній перепідготовці відповідного фахівця. Натомість, інформація про факти понаднормової праці (у тому числі при дистанційному виконанні посадових обов'язків з дому) призводить до нарахування додаткових компенсаційних і заохочувальних виплат працівникам.

Оптимізації обліку витрат на утримання працівників сприятиме використання інформації зі системи біометричної ідентифікації персоналу про реалізацію функціональних обов'язків працівниками на робочих місцях у підприємстві чи з дому. Автоматизації підлягає облік витрат на харчування працівників, експлуатацію приміщень спільного використання, загальновиробничих витрат з чітким розподілом між виробничими, адміністративними, збутовими та іншими витратами. Формування інформації про відпрацьований час та заробітну плату з використанням системи біометричної ідентифікації працівників відбувається в електронній формі та надсилається внутрішнім та зовнішнім стейкхолдерам.

10. Поступальний розвиток комунікаційних технологій формує нові вимоги до швидкості передачі даних. Використання стільникового зв'язку 4G та нової генерації 5G не здатне забезпечити інформаційні потреби користувачів технологій штучного інтелекту, тотальної віртуалізації комунікацій, безпілотності та автопілотності транспортних засобів, під'єднання до Інтернету усіх технічних пристроїв, що потребує формування концепції мобільних комунікацій 6G.

Важливою перевагою стільникового зв'язку шостого покоління є трохвимірне достовірне визначення місця перебування абонента та прямий інформаційних зв'язок між елементами стільникової мережі, що уможливлює трансформацію бухгалтерського обліку підприємств різних сфер діяльності. Зокрема, фундаментальних змін зазнає облік витрат з використанням: виробничого обладнання, під'єднаного до інформаційної системи підприємства, для перманентного своєчасного визначення собівартості промислової продукції; транспортних засобів з контрольованим пересуванням обумовленими маршрутами та превентивною ідентифікацією собівартості надання транспортних послуг; роїв безпілотних літальних апаратів для аеровізуального спостереження за виконанням сільськогосподарських та будівельних робіт з достовірним визначенням та розподілом доходів й витрат; технології підрахунку кількості відвідувачів приміщень підприємства для визначення популярності торгівельної площі та реклами з метою інформування замовників про їхню вартість.

У той же час інформаційній системі підприємств, на яких використовують стільникові мережі 6G, загрожують значні кіберризики: атаки з використанням штучного інтелекту, попередньо невідомі вразливості «нульового дня», ризики на основі квантумних обчислень, атаки з використанням швидкого (ТераГерцового) обладнання, гібридні війни тощо. Для забезпечення кіберзахисту необхідним є використання стільникових мереж 6G для моніторингу: місця перебування працівників на території чи приміщеннях підприємства; маршрутів пересування та виконання робіт транспортними засобами; доступу осіб до виробничого обладнання, будівельних майданчиків чи місць виконання сільськогосподарських робіт; присутності зловмисників у місцях вчинення правопорушень з метою запобігання втрати матеріальних та інформаційних ресурсів суб'єктів господарювання.

11. Для ефективного використання сучасних комп'ютерно-комунікаційних технологій (у тому числі наведених технологій блокчейн, Інтернету речей, стільникового зв'язку, автоматичної біометрії тощо) в обліково-безпекових процесах необхідна регламентації інформаційних

потоків підприємства. Важливими регламентуючими документами на підприємстві щодо забезпечення кіберзахисту можуть бути облікова політика підприємства та інші внутрішні документи. В обліковій політиці підприємства або в окремих внутрішніх регламентах доцільно фіксувати: перелік інформації, що є комерційною таємницею; порядок оновлення програмного забезпечення та методику інформаційної синхронізації з хмарними сервісами; здійснення зовнішніх комунікацій з користувачами інформації; порядок використання програмного і технічного забезпечення; алгоритму розподілу та застосування електронних ключів для доступу до інформації; класифікація приміщень за правом допуску та організації системи охорони території підприємства; класифікація працівників за ієрархічним рівнем доступу до інформаційних ресурсів підприємства тощо.

Інформаційний захист в умовах автоматизації обліку та управління передбачає поєднання організаційних дій працівників підприємства, які доцільно відображати в обліковій політиці та внутрішніх регламентних документах. Безпекові положення регламентації обробки облікових даних вимагають налагодження ефективного розподілу функціональних повноважень персоналу та надання прав доступу до конфіденційної інформації. Допуск до баз даних реалізується через видачу персональних цифрових підписів, логінів і паролів. Завдяки технологіям авторизації встановлюється відповідальність та відслідковуються дії персоналу щодо обробки і передачі даних.

Через відображення в обліковій політиці підприємства часових критеріїв проведення перевірок стану інформаційної безпеки, протоколів обміну даних, обмінних типів документів, сертифікатів і ліцензій на використання програмного забезпечення, гарантується надійність облікової інформації у процесі виконання обліковими та управлінськими фахівцями функціональних обов’язків.

12. З метою оптимізації інформаційних процесів менеджмент підприємства може орієнтуватися на різні форми організації обліку та кіберзахисту. Однією з організаційних форм є делегування облікових та безпекових повноважень (аутсорсинг). Передача облікової інформації та

повноважень супроводжується активними кіберзагрозами. До організаційних чинників обліку, що впливають на кібербезпеку підприємств, доцільно віднести: об'єктність, кількість працівників, невизначеність, дистанційність, комунікації з аутсорсером, комунікації з контрагентами, автоматизація, частота інформаційних актів. За виокремленими організаційними варіантами можливо оцінити імовірність прояву кіберризиків в умовах облікового аутсорсингу у розрізі його форм.

Кіберризики значно мінімізуються при делегуванні облікових повноважень хмарним сервісам обробки інформації. Але хмарний варіант делегування ускладнений в умовах необхідності перманентних комунікацій аутсорсера з менеджментом підприємства та контрагентами, що не дає змоги рекомендувати такий варіант аутсорсингу для усіх суб'єктів господарювання. Тому найбільш оптимальною формою аутсорсингу для кожного суб'єкта господарювання є варіант з мінімальною сумарною імовірністю прояву кіберризиків за усіма організаційними чинниками обліку.

13. Для оптимізації функціонування підприємств необхідним є інтегроване позиціонування аутсорсингу облікових та безпекових повноважень. Поєднане делегування функцій обліку та кіберзахисту сприятиме синергетичній мінімізації адміністративних витрат, зменшенню ймовірності прояву інформаційних та фінансових ризиків. Інтеграція аутсорсингу можлива за двома варіантами, що залежать від об'єктів та видів обліку (об'єкта модель) або організаційної структури підприємства (структурна модель).

Реалізація об'єктної моделі передбачає делегування обробки та кіберзахисту облікової інформації фінансового обліку про окремі об'єкти обліку. Оперування інформацією управлінського обліку, що може містити комерційну таємниці, відбувається лише в бухгалтерії підприємства. Відповідно до структурної організаційної моделі аутсорсинг обліково-безпекових повноважень можливий винятково щодо функціонування господарських одиниць підприємства (структурних підрозділах) із консолідацією інформації в бухгалтерії материнської компанії. У зв'язку з проявом значних кіберризиків комплексне делегування усіх обліково-

безпекових повноважень в об’єктній і структурній моделі аутсорсингу є неможливим.

Для уникнення організаційних обмежень реалізації об’єктного і структурного варіантів аутсорсингу доцільно використовувати комбіновану (мозаїчну) модель, яка полягає у мозаїчному делегуванні обліково-безпекових функцій багатьом аутсорсерам. Усі повноваження обліку та кіберзахисту поділяються на підмножини і делегуються різним аутсорсерам, які інформаційно поєднані з використанням технології блокчейн. За допомогою технології блокчейн розрізнена облікова інформація інтегрується та передається бухгалтерії і менеджменту підприємства для подальшого опрацювання. Впровадження запропонованої моделі забезпечує комплексний аутсорсинг обліково-безпекових функцій при дієвій системі кіберзахисту підприємств.

ЛІТЕРАТУРА

1. Автоматизована система контролю доступу. Матеріал з Вікіпедії – вільної енциклопедії. URL: https://uk.wikipedia.org/wiki/Автоматизована_система_контролю_доступу.

2. Александров І.А, Половян О.В. Кластеризація територіальних утворень України за рівнем економічної безпеки. Економічна кібернетика. 2000. № 5-6. С. 40–47.

3. Біометрія. Матеріал з Вікіпедії – вільної енциклопедії. URL: https://uk.wikipedia.org/wiki/ Біометрія.

4. Боримська К. П. Захист бухгалтерської інформації в обліковій політиці з метою оподаткування: організаційні аспекти. Збірник наукових праць Національного університету державної податкової служби України. 2013. № 2. С. 14-21. URL: http://nbuv.gov.ua/UJRN/znpnudps_2013_2_4.

5. Боримська К.П., Кінзерська Н.В. Концептуалізація захисту бухгалтерської інформації при міжкорпоративному електронному документообороті торговельних підприємств: проблемні аспекти. Вісник ЖДТУ. Серія: економічні науки. 2013. № 3 (65). С. 16–25. URL: http://eztuir.ztu.edu.ua/123456789/2365.

6. Бухгалтерський облік в управлінні підприємством: навчальний посібник / О.А. Лаговська, С.Ф. Легенчук, В.І. Кузь, С.В. Кучер. Житомир: Житомирський державний технологічний університет. 2017. 416 с. URL: https://learn.ztu.edu.ua/mod/resource/view.php?id=17967.

7. Вітер С. А., Світлишин І. І. Захист облікової інформації та кібербезпека підприємства. Економіка та суспільство : електрон. наук. фах. вид. 2017. № 11. С. 497–502. URL: https://economyandsociety.in.ua/journals/11_ukr/80.pdf.

8. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кіберризиків. Зовнішня торгівля: економіка, фінанси, право. 2018. № 3. С. 101–115. URL: http://nbuv.gov.ua/UJRN/uazt_2018_3_10.

9. Герасимович І. А. Організація облікової політики сучасного підприємства. Інвестиції: практика та досвід. 2018. № 7. С. 49–53. URL: http://www.investplan.com.ua/?op=1&z=6016&i=8.

10. Гончарук М.О. Комп'ютеризація бухгалтерського обліку безготівкових розрахунків. Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу. 2012. Вип. 2 (23). С. 47–51. URL: https://eztuir.ztu.edu.ua/handle/123456789/3061.

11. Горбаченко С. Кібербезпека як складова економічної безпеки України. Галицький економічний вісник, 2020. Том 66. № 5. С. 180–186. URL: https://doi.org/10.33108/galicianvisnyk_tntu2020.05.180.

12. 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.

13. Деньга С. М., Верига Ю. О. Захист інформації в комп`ютерних інформаційних системах бухгалтерського обліку. Бухгалтерський облік і аудит. 2004. № 5. С. 59–65. URL: https://lib.dsau.dp.ua/book/17336.

14. Дикий А.П., Семенчук М.В. Комерційна таємниця як складова економічної безпеки підприємства. Вісник Житомирського державного технологічного університету. Економічні науки. Житомир: ЖДТУ, 2005. № 4 (34). С. 75–82. URL: https://library.ztu.edu.ua/doccard.php/43377.

15. Євдокимов В. В. Надійність бухгалтерської інформації як передумова забезпечення економічної безпеки підприємства. Вісник ЖДТУ. 2011. № 3 (57). С. 46–50. URL: http://eztuir.ztu.edu.ua/123456789/4530.

16. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19.

17. Кирильєва Л.О., Поставний А.О. Організаційні аспекти обліку ноу-хау та комерційної таємниці в інноваційній системі підприємства. Економічна стратегія і перспективи розвитку сфери торгівлі та послуг. 2010. № 2. С. 123-130. URL: http://nbuv.gov.ua/UJRN/esprstp_2010_2_20.

18. Кібератака, вірус Petya.A і до чого тут M.E.Doc. Електронний журнал «Дебет-Кредит». URL: https://news.dtkt.ua/state/other/44158.

19. Легенчук С. Ф., Царук І. М., Назаренко Т. П. (2021). Принципи захисту даних у системі обліку: управлінські аспекти. Економіка, управління та адміністрування. № 2(96). С. 61–69. URL: https://doi.org/10.26642/ema-2021-2(96)-61-69.

20. Лобода Н. О., Чабанюк О. М., Сенишин Б. Б. Аутсорсинг як механізм облікових інновацій на українських підприємствах. Бізнес Інформ. 2020. № 2. С. 329–336. URL: https://doi.org/10.32983/2222-4459-2020-2-329-336.

21. Марчук У. Комерційна таємниця: правова регламентація, відповідальність і заходи щодо її збереження. Бухгалтерський облік і аудит. 2012. № 5. С. 49–54.

22. Мілян К.В., Грицюк Ю.І. Особливості організації інформаційної безпеки корпоративної мережі промислової компанії. Науковий вісник НЛТУ України. 2013. Вип. 23(4). С. 314–328. URL: http://nbuv.gov.ua/UJRN/nvnltu_2013_23.

23. 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. URL: http://ir.polissiauniver.edu.ua/handle/123456789/7427.

24. Муравський В. В. Комп'ютерно-комунікаційна форма обліку : монографія. Тернопіль : ТНЕУ, 2018. 486 с. URL: http://dspace.wunu.edu.ua/handle/316497/33170.

25. Муравський В. Застосування інформаційних технологій у первинному обліку торговельних, розрахункових і транспортних операцій. Вісник КНТЕУ. 2009. № 3. С. 69–76. URL: http://visnik.knute.edu.ua/files/2009/03/10.pdf.

26. Назаренко О. В., Суровицька А. В. Аутсорсинг бухгалтерського обліку: переваги, недоліки та особливості запровадження. Економіка та держава. 2018. № 12. С. 50–54. URL: https://doi.org/10.32702/2306-6806.2018.12.50.

27. Нехай В. А., Нехай В. В. Інформаційна безпека як складова економічної безпеки підприємств. Науковий вісник Міжнародного гуманітарного університету. 2017. Вип. 24(2). С. 137–140. URL: http://nbuv.gov.ua/UJRN/Nvmgu_eim_2017_24%282%29__30.

28. Перевалова Л.В., Кваша С.В. Захист конфіденційної інформації: проблеми та шляхи вирішення. Вісник Національного технічного університету «Харківський політехнічний інститут»: зб. наук. праць. Тематичний випуск: Актуальні проблеми розвитку українського суспільства. Харків: НТУ «ХПІ». 2011. № 30. 179 с.

29. Петрук О. М., Новак О. С. Сутність криптовалюти як методологічна передумова її облікового відображення. Вісник ЖДТУ. 2017. № 4 (82). С. 48-55. URL: http://nbuv.gov.ua/UJRN/Vzhdtu_econ_2017_4_11.

30. Підсумки 2018 року в цифрах. URL: https://cyberpolice.gov.ua/results/2018.

31. 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.

32. Пушкар М.С., Щирба М.Т. Теорія і практика формування облікової політики : монографія. Тернопіль : Карт-бланш, 2010. 260 с.

33. Радченко М. А. Особливості відображення електронних грошей в обліку. Науковий вісник Ужгородського університету. Серія : Економіка. 2015. Вип. 1(2). С. 121–124. URL: http://www.visnyk-ekon-old.uzhnu.edu.ua/images/pubs/45/2/45_2_121-124_Радченко.pdf.

34. Ревенок В.І., Мамчур О.С. Основні аспекти інформаційних систем з обліку нарахування заробітної плати. Молодий вчений. 2015. № 2 (17). С. 22–25. URL: http://nbuv.gov.ua/UJRN/molv_2015_2%283%29__7.

35. Рожелюк В.М. Заходи забезпечення захисту облікової інформації // Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації. 2013. № 2 (12). С. 335–340. URL: http://library.wunu.edu.ua/images/stories/praci_vukladachiv/Факультет%20ОА/Кафедра%20обліку%20в%20державному%20секторі%20економіки%20та%20сфері%20послуг/Рожелюк%20В.М/111Заходи%20забезпечення%20захисту%20облікової%20інформац.pdf.

36. Сахаров П.О. Окремі аспекти обліку електронних грошей та особливості проведення їх аналізу та аудиту у банках. Мукачівський державний університет. 2017. Випуск № 9. С. 1192–1197. URL: https://economyandsociety.in.ua/journals/9_ukr/205.pdf.

37. Сиротюк О. Право ІВ на комерційну таємницю. Баланс. 2010. № 95. С. 57–59. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/boau_2012_5_7.pdf.

38. Система обліку робочого часу «STOP-Time 4.0». К.:ТОВ «Кард-Сістемс». 2016. 62 с. URL: https://card-sys.com/data/download/Nastanova_koristuvacha_STOP-Time_4.0___.doc

39. Чухно І. С. Удосконалення класифікації користувачів звітності. Облік і фінанси. 2012. № 1. С. 85–90. URL: http://nbuv.gov.ua/UJRN/Oif_apk_2012_1_17.

40. Шишкова Н. Л. Засоби підвищення керованості безпекою облікової інформації. Економічний вісник Національного гірничого університету. 2016. № 3. С. 119–127. URL: http://nbuv.gov.ua/UJRN/evngu_2016_3_17.

41. Шпак В.А. Організація захисту облікової інформації. Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації. 2015. № 2. С. 181–187. URL : http://nbuv.gov.ua/UJRN/boaa_2015_2_27.

42. Щирська А. Ю. Вимоги користувачів до якості облікової інформації. Економічний простір. 2018. № 139. С. 213–228. URL: http://www.prostir.pdaba.dp.ua/index.php/journal/article/download/383/374.

43. Як писати і вимовляти bitcoin. URL: https://www.bbc.com/ukrainian/blog-olexandr-ponomariv-41225133.

44. Янчев А.В. Електронний облік праці та її оплати – основа державної стратегії формування людського капіталу. Вісник ХНАУ ім. В.В. Докучаєва. Серія: Економічні науки. 2015. № 2. С. 212–221.

45. Яцик Т.В. Методика фінансового обліку криптовалюти як особливого виду електронних грошей. Молодий вчений. 2017. № 2 (42). С. 349–354. URL: http://www.economy.nayka.com.ua/?op=1&z=7616.

46. Abdelwahab I., Ramadan N., Hefny H. Cybersecurity Risks of Blockchain Technology. International Journal of Computer Applications. 2020. № 177. P. 8–14. URL: https://doi.org/10.5120/ijca2020919922.

47. Aisenberg Michael, Editor Esq. State and Local ICT Policy: A Framework for Cybersecurity, IOT, Cloud, Block Chain, etc. Sub-Federal Cyber Policy. 2018. URL: https://www.researchgate.net/publication/334747029_State_and_Local_ICT_Policy_A_Framework_for_Cybersecurity_IOT_Cloud_Block_Chain_etc.

48. Alibhai Salim, Bakker Erwin, Balasubramanian T., Bharadva Kunal, Chaudhry Asif, Coetsee Danie, Johnstone Chris, Kuria Patrick, Naidoo Christopher, Ramanarayanan,J. Accounting policies, changes in accounting estimates and errors. Interpretation and Application of IFRS® Standards. Wiley. 2021. P. 117–137. URL: https://doi.org/10.1002/9781119818663.ch7.

49. Alkarawy H., AL-Kuwair E. Accounting improving the costs and business process management in transportation to a third party. Accounting. 2021. P. 701–708. URL: https://doi.org/10.5267/j.ac.2020.12.006.

50. Al-Mohammed H., Yaacoub E. On The Use of Quantum Communications for Securing IoT Devices in the 6G Era. 2021. P. 1–6. URL: https://doi.org/10.1109/ICCWorkshops50388.2021.9473793.

51. Almutairi M., Riddle S. A Framework for Managing Security Risks of Outsourced IT Projects. An Empirical Study. 2018. P. 40–44. URL: https://doi.org/10.1145/3178461.3178476.

52. Alsaqa Zeyad H., Hussein A. I., Mohammed Mahmood S. The Impact of Blockchain on Accounting Information Systems. Journal of Information Technology Management. 2020. № 11. P. 62–80. URL: https://doi.org/10.22059/jitm.2019.74301.

53. Asatiani A., Apte U., Penttinen,E., Rönkkö M., Saarinen, T. Impact of accounting process characteristics on accounting outsourcing - Comparison of users and non-users of cloud-based accounting information systems. International Journal of Accounting Information Systems. 2019. № 34. URL: https://doi.org/10.1016/j.accinf.2019.06.002.

54. Asieieva Yu. Problem questions of cyber-addictions classification. Psychology and Personality. 2020. № 2. P. 23–40. URL: https://doi.org/10.33989/2226-4078.2020.2.211910.

55. B2B cross-border transactions on blockchain in various regions worldwide in 2020 with forecasts from 2021 to 2025. Statista. https://www.statista.com/statistics/1228825/b2b-cross-border-transactions-on-blockchain-worldwide.

56. Badhwar Raj. AI for Cybersecurity. The CISO's Next Frontier. 2021. P. 41–44. URL: https://doi.org/10.1007/978-3-030-75354-2_4.

57. Bansal S. K., Batra R., Jain N. Blockchain and the future of accounting, The Management Accountant Journal. 2018. №. 6. P. 60–66. URL: https://www.researchgate.net/publication/326367568_Blockchain_The_Future_of_Accounting.

58. Baranenko R.V. Cyber attacks as a form of cyber terrorism. Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences. 2021. № 1. P. 45–50. URL: https://doi.org/10.32838/2663-5941/2021.1-1/07.

59. Benaroch M. Cybersecurity Risk in IT Outsourcing—Challenges and Emerging Realities. Information Systems Outsourcing. 2020. P. 313–334. URL: https://doi.org/10.1007/978-3-030-45819-5_13.

60. Bonson E., Bednarova M. Blockchain and its implications for accounting and auditing, Meditari Accountancy Research. 2019. Vol. 27. №. 5. P. 725–740. URL: https://doi.org/10.1108/MEDAR-11-2018-0406.

61. Boonkrong S. Biometric Authentication. Authentication and Access Control. 2021. P. 107–132. URL: https://doi.org/10.1007/978-1-4842-6570-3_5.

62. Cai C.W. Triple-entry accounting with blockchain: how far have we come? Accounting Finance. 2021. URL: https://doi.org/10.1111/acfi.12556.

63. Chesney Steve, Roy Kaushik, Khorsandroo Sajad. Machine Learning Algorithms for Preventing IoT Cybersecurity Attacks. 2021. URL: https://doi.org/10.1007/978-3-030-55190-2_53.

64. Chikutuma C. Integrated Reporting: A Story of Stakeholder Accountability. 5th International Conference on Accounting, Auditing, and Taxation (ICAAT 2016). 2016. URL: https://doi.org/10.2991/icaat-16.2016.4.

65. Concept of creation and development of 5G / IMT-2020 networks. URL: https://digital.gov.ru/uploaded/files/kontseptsiya-sozdaniya-i-razvitiya-setej-5g-imt-2020.pdf.

66. Coyne J.G., McMickle P.L. Can Blockchains serve an accounting purpose. Journal of Emerging Technologies in Accounting. 2017. Vol. 14. №. 2, P. 101–111. URL: https://doi.org/10.2308/jeta-51910.

67. Cremonini M. Cloud Security Risk Management. Cloud Computing Security. 2020. P. 95–114. URL: https://doi.org/10.1201/9780429055126-10.

68. Cullinan C., Zheng X. Accounting outsourcing and audit lag. Managerial Auditing Journal. 2017. № 32. P. 276–294. URL: https://doi.org/10.1108/MAJ-03-2016-1349.

69. Cyberthreat Defense Report / CyberEdge Group. Annapolis: CyberEdge Group, 2019. 50 p.

70. Demirkan Sebahattin, Demirkan Irem, Mckee Andrew. Blockchain technology in the future of business cyber security. Journal of Management Analytics. 2020. Vol. 7, Issue 2. P. 189–208. URL: https://doi.org/10.1080/23270012.2020.1731721.

71. Desyatnyuk O., Muravskyi V., Shevchuk O. and Oleksiiv M. Dual Use of Internet of Things Technology in Accounting Automation and Cybersecurity, 12th International Conference on Advanced Computer Information Technologies (ACIT). Spisska Kapitula, Slovakia. 26-28 September. 2022. P. 360–363. URL: https://doi.org/10.1109/ACIT54803.2022.9913080.

72. Digital resonance: the new factor influencing location attractiveness (2019). The 2019 Kearney Global Services Location Index. URL: https://www.kearney.com/digital-transformation/gsli/2019-full-report.

73. Djenna Amir, Saidouni Djamel Eddine, Wafia Abada. A Pragmatic Cybersecurity Strategies for Combating IoT-Cyberattacks. 2020. P. 1–6. URL: https://doi.org/10.1109/ISNCC49221.2020.9297251.

74. Drokina N., Kaipova Gulnara. Formation of accounting policy content. Chronos Journal. 2020. URL: https://doi.org/10.31618/2658-7556-2020-40-1-3.

75. Dupuis Marc, Renaud Karen. Scoping the ethical principles of cybersecurity fear appeals. Ethics and Information Technology. 2020. P. 1–20. URL: https://doi.org/10.1007/s10676-020-09560-0.

76. Eaton Tim, Grenier Jonathan, Layman David. Accounting and Cybersecurity Risk Management. Current Issues in Auditing. 2019. Vol. 13. No. 2. C1–C9. URL: https://doi.org/10.2308/ciia-52419.

77. El-Ebiary Y., Alawi N. The Risks of Accounting Information Systems. International Journal of Engineering Trends and Technology. 2020. P. 2231–2381. URL: https://doi.org/10.14445/22315381/CATI3P220.

78. Estimate of overall cryptocurrency market cap per week from July 2010 to June 2021. Statista. URL: https://www.statista.com/statistics/730876/cryptocurrency-maket-value.

79. Fletcher J., Gillum D., Moritz R., Schwartz A. Demographic and Salary Trends of the 2020 Biosafety Workforce. Applied Biosafety. 2020. № 3. URL: https://doi.org/10.1089/apb.20.0066.

80. Fubara-Manuel I. Biometric Capture. African Diaspora. 2020. № 12. P. 1–25. URL: https://doi.org/10.1163/18725465-01201002.

81. Georg Schaffner Laura, Grove Hugh, Holder Anthony, Clouse Mac. Cybersecurity Guidance for Accountants and Executives. Internal Auditing. 2018. Vol. 33. No. 5. P. 5–20. URL: https://www.researchgate.net/publication/330199422_Cybersecurity_Guidance_for_Accountants_and_Executives.

82. Global 5G subscription forecast 2019-2025. Statista. URL: https://www.statista.com/statistics/760275/5g-mobile-subscriptions-worldwide/

83. Global Biometrics in Workforce Management Market 2019. Data Snapshot: Biometrics in the workplace commonplace, but are they secure?

URL: https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure.

84. Global Connectivity Index – GCI Ranking Table. URL: https://www.huawei.com/minisite/gci/en/country-rankings.html.

85. Global Cybersecurity Index (GCI) 2018. ITU Publications. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

86. Global Cybersecurity Index (GCI) 2021. International Telecommunication Union. Geneva : ITUPublications, 2021. 172 p. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

87. Global Innovation Index 2018. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2018-intro5.pdf.

88. Gomaa A.A., Gomaa M.I., Stampone A. A transaction on the Blockchain: an AIS perspective, intro case to explain transactions on the ERP and the role of the internal and external auditor, Journal of Emerging Technologies in Accounting. 2019. Vol. 16. №. 1. P. 47–64. URL: https://doi.org/10.2308/jeta-52412.

89. Gupta W. Salary Estimator using Data Science. International Journal for Modern Trends in Science and Technology. 2020. № 6. P. 319–322. URL: https://doi.org/10.46501/IJMTST061259.

90. Haapamäki Elina, Sihvonen Jukka. Cybersecurity in accounting research. Managerial Auditing Journal. 2019. № 34. P. 808–834. URL: https://doi.org/10.1108/MAJ-09-2018-2004.

91. Haque Md, Haque Shameemul, Kumar Kailash, Singh Narendra. A Comprehensive Study of Cyber Security Attacks, Classification, and Countermeasures in the Internet of Things. 2021. P. 63–90. URL: https://doi.org/10.4018/978-1-7998-4201-9.ch004.

92. Harrast Steven. Robotic process automation in accounting systems. Journal of Corporate Accounting & Finance. 2020. № 31. P. 4. URL: https://doi.org/10.1002/jcaf.22457.

93. Henry Matey Akwetey, Danquah Paul, Koi-Akrofi Godfred, Asampana Isaac. Critical Infrastructure Cybersecurity Challenges: IoT in Perspective. International Journal of Network Security & Its Applications. 2021. № 13. P. 41–58. URL: https://doi.org/10.5121/ijnsa.2021.13404.

94. Hentea Mariana. Principles of Cybersecurity. Building an Effective Security Program for Distributed Energy Resources and Systems: Understanding Security for Smart Grid and Distributed Energy Resources and Systems. 2021. P. 93–127. URL: https://doi.org/10.1002/9781119070740.ch3.

95. Hoschek M. Quantum security and 6G critical infrastructure. Serbian Journal of Engineering Management. 2021. № 6. P. 1–8. URL: https://doi.org/10.5937/SJEM2101001H.

96. Huang R., Turner G. How the UK Can Lead in 5G and 6G Security and Standards. RUSI Newsbrief. Emerging Technologies. 2020. № 40(7). URL: https://doi.org/10.7945/18ch-1a56.

97. Internet of things (IoT) security threats and concerns worldwide. Statista. URL: https://www.statista.com/statistics/1202640/internet-of-things-security-concerns/

98. Internet Security Threat Report / Symantec. Mountain View: Symantec Corporation, 2019. 61 p.

99. Is cybersecurity about more than protection? EY Global Information Security Survey 2018–19. URL: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2018-19.pdf?download.

100. Janvrin Diane, Wang Tawei. Implications of Cybersecurity on Accounting Information. Journal of Information Systems. 2019. Vol. 33. No. 3. A1–A2. URL: https://doi.org/10.2308/isys-10715.

101. Kafka Sofiia. The stages of accounting policies formation. The actual problems of regional economy development. 2017. № 1. P. 156–164. URL: https://doi.org/10.15330/apred.1.13.156-164.

102. Karajovic M., Kim H.M., Laskowski M. Thinking outside the block: projected phases of Blockchain integration in the accounting industry, Australian Accounting Review. 2019. Vol. 29. №. 2. P. 319–330. URL: https://doi.org/10.2139/ssrn.2984126.

103. Kaur Gurdip, Lashkari Ziba, Habibi Lashkari Arash. Introduction to Cybersecurity. Understanding Cybersecurity Management in FinTech. 2021. P. 17–34. URL: https://doi.org/10.1007/978-3-030-79915-1_2.

104. Khan A., UL Hassan, Naveed Y., Zhao J., Niyato D., Zhang Y., Poor H. V. Blockchain and 6G: The Future of Secure and Ubiquitous Communication. 2021. ArXiv abs/2106.05673. URL: https://www.researchgate.net/publication/352308474_Blockchain_and_6G_The_Future_of_Secure_and_Ubiquitous_Communication.

105. Kim Jihyun. Accountability Policy 2.0: A New Direction of Accountability Policies Based on Every Student Succeeds Act in the U.S. The Korean Educational Administration Society. 2021. № 39. P. 69–94. URL: https://doi.org/10.22553/keas.2021.39.2.69.

106. Kohnke Anne, Shoemaker Dan. Making Cybersecurity Effective: The Five Governing Principles for Implementing Practical IT Governance and Control. EDPACS. 2015. № 52. P. 9–17. URL: https://doi.org/10.1080/07366981.2015.1087799.

107. Kokina J., Mancha R., Pachamanova D. Blockchain: emergent industry adoption and implications for accounting, Journal of Emerging Technologies in Accounting. 2017. Vol. 14. №. 2. P. 91–100. URL: https://doi.org/10.2308/jeta-51911.

108. Kozlowski S. An audit ecosystem to support Blockchain-based accounting and assurance book continuous auditing: theory and application, Continuous Auditing: Theory and Application (Rutgers Studies in Accounting Analytics), Emerald Publishing, Bingley. 2018. P. 299–313. URL: https://doi.org/10.1108/978-1-78743-413-420181015.

109. Kumar Gautam, Singh Om Prakash, Saini Hemraj. Cybersecurity: Ambient Technologies, IoT, and Industry 4.0 Implications. 2021. URL: https://doi.org/10.1201/9781003145042.

110. Kuo Jong-Yih, Liu Chien-Hung, Lin Hui-Chi. Building Graduate Salary Grading Prediction Model Based on Deep Learning. Intelligent Automation & Soft Computing. 2021. № 27. P. 53–68. URL: https://doi.org/10.32604/iasc.2021.014437.

111. Kuzlu Murat, Fair Corinne, Güler Özgür. Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things. 2021. № 1. URL: https://doi.org/10.1007/s43926-020-00001-4.

112. Lagovska Olena, Loskorikh Gabriella. Formation of Accounting Policy in IT Enterprises. Modern Economics. 2020. № 19. P. 108–113. URL: https://doi.org/10.31521/modecon.V19(2020)-18.

113. Lee GyungMin, Shim ShinWoo, Cho ByoungMo, Kim TaeKyu, Kim Kyounggon. The Classification Model of Fileless Cyber Attacks. Journal of KIISE. 2020. № 47. P. 454–465. URL: https://doi.org/10.5626/JOK.2020.47.5.454.

114. Lehenchuk S. F., Horodysky M. P., Maistrenko N. M. Protection of Accounting Data in the Conditions of Using Internet of Things: Problems and Prospects of Accounting Digitalization. Oblik i Finansi. 2021. № 91. P. 12–19. URL: https://doi.org/10.33146/2307-9878-2021-1(91)-12-19.

115. Li B., Ponson G., Ezzahi Y. Biometrics Security. 2020. URL: https://doi.org/10.13140/RG.2.2.26699.41766.

116. Liu M., Wu K. and Xu J. How will Blockchain technology impact auditing and accounting: permissionless vs. permissioned Blockchain. Current Issues in Auditing. 2019. Vol. 13. №. 2. P. 19–29. URL: https://doi.org/10.2308/ciia-52540.

117. Liu Z., Wu L., Ke J., Qu W., Wang W., Wang H. Accountable Outsourcing Location-Based Services With Privacy Preservation. IEEE Access. 2019. URL: https://doi.org/10.1109/ACCESS.2019.2936582.

118. Lu Yang. Security in 6G: The Prospects and the Relevant Technologies. Journal of Industrial Integration and Management. 2020. № 5. P. 271–289. URL: https://doi.org/10.1142/S2424862220500165.

119. Main incidents in the EU and worldwide. ENISA Threat Landscape. URL: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents.

120. Marasigan R. The Role of Ideas that shape the Institutional Change in Cybersecurity: Economic barriers of cyber-attacks. Policy in a Changing World Tackling Global Issues At: Roppongi, Tokyo Japan. 2019. URL: https://doi.org/10.6084/m9.figshare.12086763.

121. Martyniuk T. The Informative Function of Accounting in Outsourcing of the Financial and Accounting Services. Zeszyty Naukowe Uniwersytetu Szczecińskiego Finanse Rynki Finansowe Ubezpieczenia. 2016. № 2. P. 151–157. URL: https://doi.org/10.18276/frfu.2016.2.80/2-16.

122. Maszczak T. Accounting Outsourcing In Micro And Small Entities − Opportunities And Threats. Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. 2019. № 63. P. 92–107. URL: https://doi.org/10.15611/pn.2019.8.07.

123. Mercado-Velazquez Andres, Escamilla-Ambrosio P. Jorge, Ortiz-Rodriguez Floriberto. A Moving Target Defense Strategy for Internet of Things Cybersecurity. IEEE Access. 2021. P. 1–10. URL: https://doi.org/10.1109/ACCESS.2021.3107403.

124. Mobile broadband subscriptions worldwide 2007-2020. Statista. URL: https://www.statista.com/statistics/273016/number-of-mobile-broadband-subscriptions-worldwide-since-2007.

125. Mobile technology share by generation 2016-2025. Statista. URL: https://www.statista.com/statistics/740442/worldwide-share-of-mobile-telecommunication-technology/

126. Muravskyi V., Denchuk P., Reveha O. Accounting and audit of electronic transactions in metaverses. Herald of Economics. 2022. № 2. P. 128–141. URL: https://doi.org/10.35774/visnyk2022.02.128.

127. Muravskyi V., Khoma N., Khokhlova L., Chengyu L. Open document flow based on blockchane technology for cyber security of the accounting system. Herald of Economics. 2022. № 4. P. 156–170. URL: https://doi.org/10.35774/visnyk2021.04.156.

128. Muravskyi V., Muravskyi V., Shevchuk O. Classification of stakeholders (users) of accounting information for the enterprise cybersecurity purposes. Herald of Economics. 2021. № 1(99). P. 83–96. URL: https://doi.org/10.35774/visnyk2021.01.083

129. Muravskyi V., Pochynok N., Farion V. Classification of cyber risks in accounting. Herald of Economics. 2021. № 2. P. 129–144. URL: https://doi.org/10.35774/visnyk2021.02.129.

130. Muravskyi V., Pochynok N., Reveha O., Chengyu L. Accounting and control of foreign economic electronic transactions using cryptocurrencies. Herald of Economics. 2023. № 4. P. 44–60. URL: https://doi.org/10.35774/visnyk2022.04.044.

131. Muravskyi V., Shevchuk O., Muravskyi V., Lapsinskyi V. Improving the accounting policy of the enterprise for its cyber protection. Herald of Economics. 2022. № 1. P. 97–109. URL: https://doi.org/10.35774/visnyk2022.01.097.

132. Muravskyi V., Zadorozhnyi Z.-M., Lytvynenko V., Yurchenko O., Koshchynets M. Comprehensive use of 6G cellular technology accounting activity costs and cyber security. Independent Journal of Management & Production (Special Edition ISE, S&P). 2022. Vol. 13 № 3. P. 107–122. URL: https://doi.org/10.14807/ijmp.v13i3.1902.

133. Mustafa Nasir. Cyber Risk and Covid-19: Managing Cyber Risks Arising From The Pandemic. Brighttalk Webinar Series. Project: Coronavirus CoV-19 to CoV-20 Pro. 2020. 10.13140/RG.2.2.12218.82886.

134. Nassimbeni G., Sartor M., Dus D. Security risks in service offshoring and outsourcing. Industrial Management and Data Systems. 2012. № 112. URL: https://doi.org/10.1108/02635571211210059.

135. Neil G. Accounting for Employee Benefits. Counting the Poor: New Thinking About European Poverty Measures and Lessons for the United States. 2012. URL: https://doi.org/10.1093/acprof:oso/9780199860586.003.0007.

136. Nicholson B., Aman A. Managing attrition in offshore finance and accounting outsourcing: Exploring the interplay of competing institutional logics. Strategic Outsourcing: An International Journal. 2012. № 5. URL: https://doi.org/10.1108/17538291211291765.

137. Number of Blockchain wallet users worldwide. Statista. URL: https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/

138. Number of cryptocurrencies worldwide from 2013 to 2021. Statista. URL: https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

139. O'Leary D.E. Configuring blockchain architectures for transaction information in blockchain consortiums: the case of accounting and supply chain systems, Intelligent Systems in Accounting, Finance and Management. 2017. Vol. 24 №. 4. P. 138–147. URL: https://doi.org/10.1002/isaf.1417.

140. Ocheretko L., Udovychenko H. Improvement of Salary Accounting at the Enterprise. Efektyvna ekonomika. 2020. № 12. URL: https://doi.org/10.32702/2307-2105-2020.12.101.

141. Patterson W., Gergely M. Economic Prospect Theory Applied to Cybersecurity. Advances in Human Factors in Cybersecurity. 2020. P. 113-121. URL: https://doi.org/10.1007/978-3-030-52581-1_15.

142. 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.

143. Pimentel E., Bouliann E. Blockchain in Accounting Research and Practice: Current Trends and Future Opportunities. Accounting Perspectives. 2019. № 19 (3). P. 325–361. URL: https://doi.org/10.1111/1911-3838.12239.

144. Popovski P., Chiariotti F., Huang K., Kalør A., Kountouris M., Pappas N., Soret B. A Perspective on Time towards Wireless 6G. 2021. URL: https://arxiv.org/abs/2106.04314.

145. Porambage P., Gür G., Osorio D. P. M., Liyanage M., Gurtov A., Ylianttila M. The R-oadmap to 6G Security and Privacy. IEEE Open Journal of the Communications Society. 2021. vol. 2. P. 1094–1122. URL: https://doi.org/10.1109/OJCOMS.2021.3078081.

146. Prakash Febin, Baskar Kala, Sadawarti Harsh. Cyber Crime: Challenges and its Classification. International Multi-disciplinary Academic Research Conference (IMARC-2019). 2019. P. 2–4. URL: https://www.researchgate.net/publication/336115866_Cyber_Crime_Challenges_and_its_Classification.

147. Rajput B. Exploring the Phenomenon of Cyber Economic Crime. Cyber Economic Crime in India. 2020. P. 53–78. URL: https://doi.org/10.1007/978-3-030-44655-0_4.

148. Rasche A., Esser D. From Stakeholder Management to Stakeholder Accountability. Journal of Business Ethics. 2006. № 65. P. 251–267. URL: https://doi.org/10.1007/s10551-005-5355-y.

149. Rındasu S.M. Blockchain in accounting: trick or treat? Quality Access to Success. 2019. Vol. 20. №. 170 P. 143–147. URL: https://www.researchgate.net/publication/333249353_Blockchain_in_accounting_Trick_or_treat.

150. Risk committees. The Institute of Chartered Accountants in England and Wales. URL: https://www.icaew.com/technical/corporate-governance/committees/risk-committees.

151. Rodrigues B., Franco M., Parangi G., Stiller B. SEConomy: A Framework for the Economic Assessment of Cybersecurity. Economics of Grids, Clouds, Systems, and Services, 16th International Conference, GECON 2019, Leeds, UK, September 17–19, 2019. P. 154–166. URL: https://doi.org/10.1007/978-3-030-36027-6_13.

152. Rohan Rohani, Funilkul Suree, Pal Debajyoti, Thapliyal Himanshu. Humans in the Loop: Cybersecurity Aspects in the Consumer IoT Context. IEEE Consumer Electronics Magazine. 2021. № 99. P. 1–10. URL: https://doi.org/10.1109/MCE.2021.3095385.

153. Rosenzweig Paul. 10 Conservative Principles for Cybersecurity Policy. The Heritage Foundation for Leadership of America. 2011. 2513. URL: http://thf_media.s3.amazonaws.com/2011/pdf/bg2513.pdf.

154. Rue R., Pfleeger S. Making the Best Use of Cybersecurity Economic Models. Security & Privacy, IEEE. 2009. № 7. P. 52–60. URL: https://doi.org/10.1109/MSP.2009.98.

155. Samudrage D., Jayewardene D. Post-Implementation Benefits and Challenges of the Balanced Scorecard: Evidence from the Finance and Accounting Outsourcing Sector. 2019. № 10. P. 86–99. URL: https://doi.org/10.7176/RJFA/10-22-10.

156. Sarkar S. Blockchain accounting the disruption ahead. The Management Accountant Journal. 2018. Vol. 6. P. 73 https://doi.org/78. URL: https://www.researchgate.net/publication/348845098_Blockchain_Accounting_-_The_Disruption_Ahead.

157. Saydjari O. Engineering trustworthy systems: A principled approach to cybersecurity. Communications of the ACM. 2019. № 62. P. 63–69. https://doi.org/10.1145/3282487.

158. Schmitt Michael. Classification of Cyber Conflict. Journal of Conflict and Security Law. 2012. № 17 (2). 245–260. URL: https://doi.org/10.1093/jcsl/krs018.

159. Schmitz J., Leoni G. Accounting and auditing at the time of Blockchain technology: a research agenda, The Management Accountant Journal. 2019. Vol. 29. №. 2. P. 331–342. URL: https://doi.org/10.1111/auar.12286.

160. Sectoral thematic threat analysis ETL2020. ENISA Threat Landscape. European Union Agency for Cybersecurity. URL : https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis/at_download/fullReport.

161. Seo Jinsil, Bruner Michael, Payne Austin, Gober Nathan, McMullen Donald, Chakravorty Dhruva. Using Virtual Reality to Enforce Principles of Cybersecurity. The Journal of Computational Science Education. 2019. № 10. P. 81–87. URL: https://doi.org/10.22369/issn.2153-4136/10/1/13.

162. Sheehan Barry, Murphy Finbarr, Kia Arash, Kiely Ronan. A quantitative bow-tie cyber risk classification and assessment framework. Journal of Risk Research. 2021. P. 1–20. URL: https://doi.org/10.1080/13669877.2021.1900337.

163. Sheldon M.D. Using Blockchain to aggregate and share misconduct issues across the accounting profession. Current Issues in Auditing. 2019. Vol. 12. №. 2. P. 27–35. URL: https://doi.org/10.2308/ciia-52184.

164. Šikanjić Nedeljko, Avramović Zoran, Marinković Dražen. Cybersecurity IoT Architecture: One Proposed Solution for the Security Risks and Threats. The 1st International Conference on Maritime Education and Development. 2021. P. 325–331. URL: https://doi.org/10.1007/978-3-030-64088-0_29.

165. Sinha S. Blockchain – opportunities and challenges for accounting professionals, Journal of Corporate Accounting and Finance. 2019. Vol. 31. P. 65–67. URL: https://doi.org/10.1002/jcaf.22430.

166. Sinno S., Hawley C. How biometrics can save companies from ‘fire and forget’. Biometric Technology Today. 2020. № 7. P. 5–8. URL: https://doi.org/10.1016/S0969-4765(20)30095-3.

167. Siriwardhana Y., Porambage P., Liyanage M., Ylianttila M. AI and 6G Security: Opportunities and Challenges. Joint European Conference on Networks and Communications (EuCNC) & 6G Summit. Porto, Portugal. 2021. URL: https://www.researchgate.net/publication/350824466_AI_and_6G_Security_Opportunities_and_Challenges.

168. Size of the Internet of Things (IoT) security market worldwide from 2016 to 2025. Statista. URL: https://www.statista.com/statistics/993789/worldwide-internet-of-things-security-market-size/

169. Smith E. How will IoT benefit the accounting profession? 2020. URL: https://www.itproportal.com/features/how-will-iotbenefit-the-accounting-profession.

170. Smith Kane, Dhillon Gurpreet, Carter Lemuria. User values and the development of a cybersecurity public policy for the IoT. International Journal of Information Management. 2021. № 56. URL: https://doi.org/10.1016/j.ijinfomgt.2020.102123.

171. Sofiah Aman A., Maelah R., Amiruddin R., Hamzah N. Management control in accounting outsourcing services. Business Strategy Series. 2013. № 14. P. 43–49. URL: https://doi.org/10.1108/17515631311325097.

172. Spitters Thomas Heaton CPA. A Supplement to Cybersecurity Breviary for Accountants Kindle Edition. Baume Verlag, San Francisco. 2019. 61 p.

173. Steingartner William, Galinec Darko. Cyber Threats and Cyber Deception in Hybrid Warfare. Acta Polytechnica Hungarica. 2021. № 18. P. 25–45. URL: https://doi.org/10.12700/APH.18.3.2021.3.2.

174. Stitilis D., Rotomskis I., Laurinaitis M., Nadvynychnyy S., Khorunzhak N. National Cybersecurity Strategies: Management, Unification and

Assessment. Independent Journal of Management & Production. 2020. № 11 (9). P. 2341–2354. URL: https://doi.org/10.14807/ijmp.v11i9.1431.

175. Strupczewski Grzegorz. Defining cyber risk. Safety Science. 2021. № 6. P. 135. URL: https://doi.org/10.1016/j.ssci.2020.105143.

176. Summary Report / Telstra Security Report 2019. Paddington : Telstra Corporation Limited, 2019. 19 p.

177. Sun Zhenjun, Li Qi, Liu Yunfan, Zhu Yuhao. Opportunities and Challenges for Biometrics. China's e-Science Blue Book 2020. 2021. P. 101–125. URL: https://doi.org/10.1007/978-981-15-8342-1_6.

178. Tan B.S., Low K.Y. Blockchain as the database engine in the accounting system, Australian Accounting Review. 2019. Vol. 29. №. 2. P. 312–318. URL: https://doi.org/10.1111/auar.12278.

179. The 2019 Kearney Global Services Location Index. Digital resonance: the new factor influencing location attractiveness. URL: https://www.kearney.com/digital-transformation/gsli/2019-full-report.

180. Tiron Tudor A., Deliu D., Farcane N., Donțu A. Managing change with and through blockchain in accountancy organizations: a systematic literature review. Journal of Organizational Change Management. ahead-of-print. 2021. URL: https://doi.org/10.1108/JOCM-10-2020-0302.

181. Tsimperidis Ioannis, Yucel Cagatay, Katos Vasilios. Age and Gender as Cyber Attribution Features in Keystroke Dynamic-Based User Classification Processes. Electronics. 2021. № 10. P. 835. URL: https://doi.org/10.3390/electronics10070835.

182. Value of cryptocurrency theft worldwide from 2016 to 2020. Statista. URL: https://www.statista.com/statistics/960226/theft-of-cryptocurrency-value/

183. Wang M., Zhu T., Zhang T., Zhang J., Yu S., Zhou W. Security and privacy in 6G networks: New areas and new challenges. Digital Communications and Networks. 2020. № 6. URL: https://doi.org/10.1016/j.dcan.2020.07.003.

184. Wilson K., Hugh J. Cybersecurity Economics: How Much Cybersecurity is Enough? Australian intellectual property journal. 2014. P. 7–9. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/

185. World Digital Competitiveness Ranking IMD 2018. URL: https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2018.

186. Worldwide spending on blockchain solutions from 2017 to 2025. Statista. URL: https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/

187. Wu J., Xiong F., Li C. Application of internet of Things and blockchain technologies toimprove accounting, IEEE Access. 2019. Vol. 20. P. 1–10. URL: https://doi.org/10.1109/ACCESS.2019.2930637.

188. Ylianttila M., Kantola R., Gurtov A., Mucchi L., Oppermann I. (Eds.). 6G White Paper: Research Challenges For Trust, Security And Privacy [White paper]. (6G Research Visions, No. 9). University of Oulu. 2020. URL: http://urn.fi/urn:isbn:9789526226804.

189. Zadorozhnyi Z. -M., Muravskyi V. and Shevchuk O. Influence of Organizational Factors and Forms of Accounting Outsourcing on Enterprise Cybersecurity. 11th International Conference on Advanced Computer Information Technologies (ACIT). 2021. P. 540–543. URL: https://doi.org/10.1109/ACIT52158.2021.9548370.

190. Zadorozhnyi Z. -M., Muravskyi V., Muravskyi V. and Pochynok N. Transformation of Accounting Methods with the Use of Robotic Equipment with Artificial Intelligence, 12th International Conference on Advanced Computer Information Technologies (ACIT). Spisska Kapitula, Slovakia. 2022. 26-28 September. P. 285–289. https://doi.org/10.1109/ACIT54803.2022.9912753.

191. Zadorozhnyi Z.-M., Muravskiy V., Shevchuk O. Bryk M. (2021). Innovative Accounting Methodology of Ensuring the Interaction of Economic

and Cybersecurity of Enterprises. Marketing and Management of Innovations. 2021. № 4. P. 36–46. URL: http://doi.org/10.21272/mmi.2021.4-03.

192. Zadorozhnyi Z.-M., Muravskyi V. and Muravskyi V. Combined Outsourcing of Accounting and Cybersecurity Authorities, 11th International Conference on Advanced Computer Information Technologies (ACIT). 2021. P. 544–547. URL: https://doi.org/10.1109/ACIT52158.2021.9548649.

193. Zadorozhnyi Z.-M., Muravskyi V., Shevchuk O. Management accounting of electronic transactions with the use of cryptocurrencies. Financial And Credit Activity: Problems Of Theory And Practice. 2018. № 3(26). P. 169–177. URL: http://dx.doi.org/10.18371/fcaptp.v3i26.144368.

194. Zadorozhnyi Z.-M., Muravskyi V., Shevchuk O. Rusin V., Akimjaková B., Gažiová M. Intelligent behavioural analysis of social network data for the purposes of accounting and control, 12th International Conference on Advanced Computer Information Technologies (ACIT). Spisska Kapitula, Slovakia. 2022. 26-28 September. P. 276–280. URL: https://doi.org/10.1109/ACIT54803.2022.9913136.

195. 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). 149–157. URL: https://doi.org/10.18371/fcaptp.v3i34.215462.

196. Zadorozhnyi Z.-M., Ometsinska I., & Muravskyi V. Determinants of Firm's Innovation: Increasing the Transparency of Financial Statements. Marketing and Management of Innovations. 2021. № 2. P. 74–86. URL: http://doi.org/10.21272/mmi.2021.2-06.

197. Zadorozhnyi Z.-M., Sudyn Y., Muravskyi V. Goodwill Assessment in Enterprise Management: Innovative Approaches Using Computer and Communication Technologies. Marketing and Management of Innovations. 2018. 4. P. 43–53. URL: http://doi.org/10.21272/mmi.2018.4-04.

198. Zadorozhnyy Z.-M., Muravskiy V., Yatsyshyn S., Shevchuk O. Accounting of wages with the use of biometrics to ensure cybersecurity of

enterprises. Financial and Credit Activity: Problems of Theory and Practice. 2021. 3(38). P. 162–172. URL: https://doi.org/10.18371/fcaptp.v3i38.237446.

199. Zhang J., Wang Z., Wang D., Zhang X., Gupta B B., Liu X., Ma J. A Secure Decentralized Spatial Crowdsourcing Scheme for 6G-Enabled Network in Box. IEEE Transactions on Industrial Informatics. 2021. 1–11. URL: https://doi.org/10.1109/TII.2021.3081416.

200. Zoidze D. R. The Outsourcing and Peculiarities of Its Application in the Pharmaceutical Industry Sector. Business Inform. 2017. № 5. P. 274–278. URL: https://www.business-inform.net/export_pdf/business-inform-2017-5_0-pages-274_278.pdf.

ДОДАТКИ

Додаток А

Глобальний рейтинг кібербезпеки країн у 2020 році

Назва країни	Оцінка	Рейтинг
США	100	1
Об'єднане Королівство	99.54	2
Саудівська Аравія	99.54	2
Естонія	99.48	3
Корея (Респ.)	98.52	4
Сінгапур	98.52	4
Іспанія	98.52	4
Російська Федерація	98.06	5
Об'єднані Арабські Емірати	98.06	5
Малайзія	98.06	5
Литва	97.93	6
Японія	97.82	7
Канада	97.67	8
Франція	97.6	9
Індія	97.5	10
Туреччина	97.49	11
Австралія	97.47	12
Люксембург	97.41	13
Німеччина	97.41	13
Португалія	97.32	14
Латвія	97.28	15
Нідерланди	97.05	16
Норвегія	96.89	17
Маврикій	96.89	17
Бразилія	96.6	18
Бельгія	96.25	19
Італія	96.13	20
Оман	96.04	21
Фінляндія	95.78	22
Єгипет	95.48	23
Індонезія	94.88	24
В'єтнам	94.59	25
Швеція	94.55	26
Катар	94.5	27
Греція	93.98	28
Австрія	93.89	29
Польща	93.86	30
Казахстан	93.15	31
Данія	92.6	32
Китай	92.53	33

Назва країни	Оцінка	Рейтинг
Хорватія	92.53	33
Словаччина	92.36	34
Угорщина	91.28	35
Ізраїль	90.93	36
Танзанія	90.58	37
Північна Македонія	89.92	38
Сербія	89.8	39
Азербайджан	89.31	40
Кіпр	88.82	41
Швейцарія	86.97	42
Гана	86.69	43
Таїланд	86.5	44
Туніс	86.23	45
Ірландія	85.86	46
Нігерія	84.76	47
Нова Зеландія	84.04	48
Мальта	83.65	49
Марокко	82.41	50
Кенія	81.7	51
Мексика	81.68	52
Бангладеш	81.27	53
Іран (Ісламська Республіка)	81.07	54
Грузія	81.06	55
Бенін	80.06	56
Руанда	79.95	57
Ісландія	79.81	58
Південна Африка	78.46	59
Бахрейн	77.86	60
Філіппіни	77	61
Румунія	76.29	62
Молдова	75.78	63
Уругвай	75.15	64
Кувейт	75.07	65
Домініканська Республіка	75.05	66
Словенія	74.93	67
Чеська Республіка	74.37	68
Монако	72.57	69
Узбекистан	71.11	70
Йорданія	70.96	71
Уганда	69.98	72

Назва країни	Оцінка	Рейтинг
Замбія	68.88	73
Чилі	68.83	74
Кот д'Івуар	67.82	75
Коста-Ріка	67.45	76
Болгарія	67.38	77
Україна	65.93	78
Пакистан	64.88	79
Албанія	64.32	80
Колумбія	63.72	81
Куба	58.76	82
Киргизстан	49.64	92
Камерун	45.63	93
Непал (Республіка)	44.99	94
Чад	40.44	95
Буркіна Фасо	39.98	96
Малаві	36.83	97
Зімбабве	36.49	98
М'янма	36.41	99
Сенегал	35.85	100
Ліхтенштейн	35.15	101
Судан	35.03	102
Панама	34.11	103
Алжир	33.95	104
Йти	33.19	105
Ямайка	32.53	106
Гамбія	32.12	107
Сурінам	31.2	108
Ліван	30.44	109
Боснія і Герцеговина	29.44	110
Самоа	29.33	111
Фіджі	29.08	112
Лівія	28.78	113
Гайана	28.11	114
Ефіопія	27.74	115
Венесуела	27.06	116
Андорра	26.38	117
Папуа-Нова Гвінея	26.33	118
Еквадор	26.3	119
Монголія	26.2	120
Сьєрра-Леоне	25.31	121
Держава Палестина	25.18	122
Мозамбік	24.18	123
Мадагаскар	23.33	124
Тринідад і Тобаго	22.18	125
Сирійська Арабська Республіка	22.14	126

Назва країни	Оцінка	Рейтинг
Науру	21.42	127
Тонга	20.95	128
Ірак	20.71	129
Гвінея	20.53	130
Лаоська ПДР	20.34	131
Камбоджа	19.12	132
Мавританія	18.94	133
Бутан	18.34	134
Есватіні	18.23	135
Кабо Верде	17.74	136
Сомалі	17.25	137
Таджикистан	17.1	138
Барбадос	16.89	139
Болівія (Багатонаціональна Держава)	16.14	140
Сан-Томе і Принсіпі	15.64	141
Антигуа і Барбуда	15.62	142
Конго (Республіка)	14.72	143
Туркменістан	14.48	144
Кірібаті	13.84	145
Сан-Марино	13.83	146
Багамські острови	13.37	147
Сальвадор	13.3	148
Сейшельські острови	13.23	149
Гватемала	13.13	150
Ангола	12.99	151
Вануату	12.88	152
Сент-Кітс і Невіс	12.44	153
Сент-Вінсент і Гренадини	12.18	154
Намібія	11.47	155
Нігер	11.38	156
Габон	11.36	157
Сент-Люсія	10.96	158
Беліз	10.29	159
Малі	10.14	160
Гвінея-Бісау	9.85	161
Ліберія	9.72	162
Гренада	9.41	163
Лесото	9.08	164
Нікарагуа	9	165
Соломонові острови	7.08	166
Гаїті	6.4	167
Тувалу	5.78	168
Південний Судан	5.75	169

Назва країни	Оцінка	Рейтинг
Дем. Республіка Конго	5.3	170
Афганістан	5.2	171
Маршаллові острови	4.9	172
Тимор-Лешті	4.26	173
Домініка	4.2	174
Коморські острови	3.72	175
Центральноафрикансь ка Республіка	3.24	176
Мальдіви	2.95	177

Назва країни	Оцінка	Рейтинг
Гондурас	2.2	178
Джібуті	1.73	179
Бурунді	1.73	179
Еритрея	1.73	179
Екваторіальна Гвінея	1.46	180
Дем. Корейська Народна Республіка	1.35	181
Мікронезія	0	182
Ватикан	0	182
Ємен	0	182

Джерело: Global Cybersecurity Index 2020. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

Додаток Б

Глобальний рейтинг країн за рівнем інноваційності у 2020 та 2023 рр.

Рейтинг у 2023 р.	Рейтинг у 2020 р.	Країна	Оцінка	Місце в групі дохідності
1	1	Швейцарія	67.6	1
2	2	Швеція	64.2	2
3	3	США	63.5	3
4	4	Об'єднане Королівство	62.4	4
5	8	Сінгапур	61.5	5
6	7	Фінляндія	61.2	6
7	5	Нідерланди (Королівство)	60.4	7
8	9	Німеччина	58.8	8
9	6	Данія	58.7	9
10	10	Республіка Корея	58.6	10
11	12	Франція	56.0	11
12	14	Китай	55.3	1
13	16	Японія	54.6	12
14	13	Ізраїль	54.3	13
15	17	Канада	53.8	14
16	25	Естонія	53.4	15
17	11	Гонконг, Китай	53.3	16
18	19	Австрія	53.2	17
19	20	Норвегія	50.7	18
20	21	Ісландія	50.7	19
21	18	Люксембург	50.6	20
22	15	Ірландія	50.4	21
23	22	Бельгія	49.9	22
24	23	Австралія	49.7	23
25	27	Мальта	49.1	24
26	28	Італія	46.6	25
27	26	Нова Зеландія	46.6	26
28	29	Кіпр	46.3	27
29	30	Іспанія	45.9	28
30	31	Португалія	44.9	29
31	24	Чеська Республіка	44.8	30
32	34	Об'єднані Арабські Емірати	43.2	31
33	32	Словенія	42.2	32
34	40	Литва	42.0	33
35	35	Угорщина	41.3	34
36	33	Малайзія	40.9	2
37	36	Латвія	39.7	35
38	37	Болгарія	39.0	3
39	51	Туреччина	38.6	4
40	48	Індія	38.1	1
41	38	Польща	37.7	36
42	43	Греція	37.5	37
43	44	Таїланд	37.1	5
44	41	Хорватія	37.1	38
45	39	Словаччина	36.2	39
46	42	В'єтнам	36.0	2
47	46	Румунія	34.7	40
48	66	Саудівська Аравія	34.5	41
49	62	Бразилія	33.6	6
50	70	Катар	33.4	42
51	47	Російська Федерація	33.3	7
52	54	Чилі	33.3	43
53	53	Сербія	33.1	8
54	57	Північна Македонія	33.0	9
55	45	Україна	32.8	3
56	50	Філіппіни	32.2	4
57	52	Маврикій	32.1	10
58	55	Мексика	31.0	11
59	60	Південна Африка	30.4	12
60	59	Республіка Молдова	30.3	13
61	85	Індонезія	30.3	5
62	67	Іран (Ісламська Республіка)	30.1	6
63	69	Уругвай	30.0	44
64	78	Кувейт	29.9	45
65	63	Грузія	29.9	14
66	68	Колумбія	29.4	15
67	79	Бахрейн	29.1	46
68	58	Монголія	28.8	7
69	84	Оман	28.4	47
70	75	Марокко	28.4	8
71	81	Йорданія	28.2	16
72	61	Вірменія	28.0	17
73	80	Аргентина	28.0	18
74	56	Коста-Ріка	27.9	19
75	49	Чорногорія	27.8	20
76	76	Перу	27.7	21
77	74	Боснія і Герцеговина	27.1	22

Рейтинг у 2023 р.	Рейтинг у 2020 р.	Країна	Оцінка	Місце в групі дохідності
78	72	Ямайка	27.1	23
79	65	Туніс	26.9	9
80	64	Білорусь	26.8	24
81	77	Казахстан	26.7	25
82	93	Узбекистан	26.2	10
83	83	Албанія	25.4	26
84	73	Панама	25.3	48
85	89	Ботсвана	24.6	27
86	96	Єгипет	24.2	11
87	71	Бруней Даруссалам	23.5	49
88	107	Пакистан	23.3	12
89	82	Азербайджан	23.3	28
90	101	Шрі Ланка	23.3	13
91	100	Кабо Верде	23.3	14
92	87	Ліван	23.2	15
93	102	Сенегал	22.5	16
94	90	Домініканська республіка	22.4	29
95	92	Сальвадор	21.8	17
96	104	Намібія	21.8	30
97	105	Болівія	21.4	18
98	97	Парагвай	21.4	31
99	108	Гана	21.3	19
100	86	Кенія	21.2	20
101	110	Камбоджа	20.8	21
102	98	Тринідад і Тобаго	20.7	50
103	91	Руанда	20.6	1
104	99	Еквадор	20.5	32
105	116	Бангладеш	20.2	22

Рейтинг у 2023 р.	Рейтинг у 2020 р.	Країна	Оцінка	Місце в групі дохідності
106	94	Киргизстан	20.2	23
107	115	Мадагаскар	19.1	2
108	95	Непал	18.8	24
109	117	Нігерія	18.4	25
110	113	Лаоська Народно-Демократична Республіка	18.3	26
111	109	Таджикистан	18.3	27
112	112	Кот д'Івуар	18.2	28
113	88	Об'єднана Республіка Танзанія	17.4	29
114	124	Того	16.9	3
115	-	Нікарагуа	16.9	30
116	103	Гондурас	16.7	31
117	120	Зімбабве	16.5	32
118	122	Замбія	16.4	4
119	121	Алжир	16.1	33
120	126	Бенін	16.0	34
121	114	Уганда	16.0	5
122	106	Гватемала	15.8	33
123	119	Камерун	15.3	35
124	118	Буркіна Фасо	14.5	6
125	127	Ефіопія	14.3	7
126	124	Мозамбік	13.6	8
127	-	Мавританія	13.5	36
128	130	Гвінея	13.3	9
129	123	Малі	12.9	10
130	-	Бурунді	12.5	11
131	128	Нігер	12.4	12
132	-	Ангола	10.3	37

Джерело:

Global Innovation Index 2020. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020.pdf.

Global Innovation Index 2023. URL:

https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2023-section1-en-gii-2023-at-a-glance-global-innovation-index-2023.pdf

Додаток В

Глобальний рейтинг країн за рівнем під'єднання до мережі Інтернет у 2020 р.

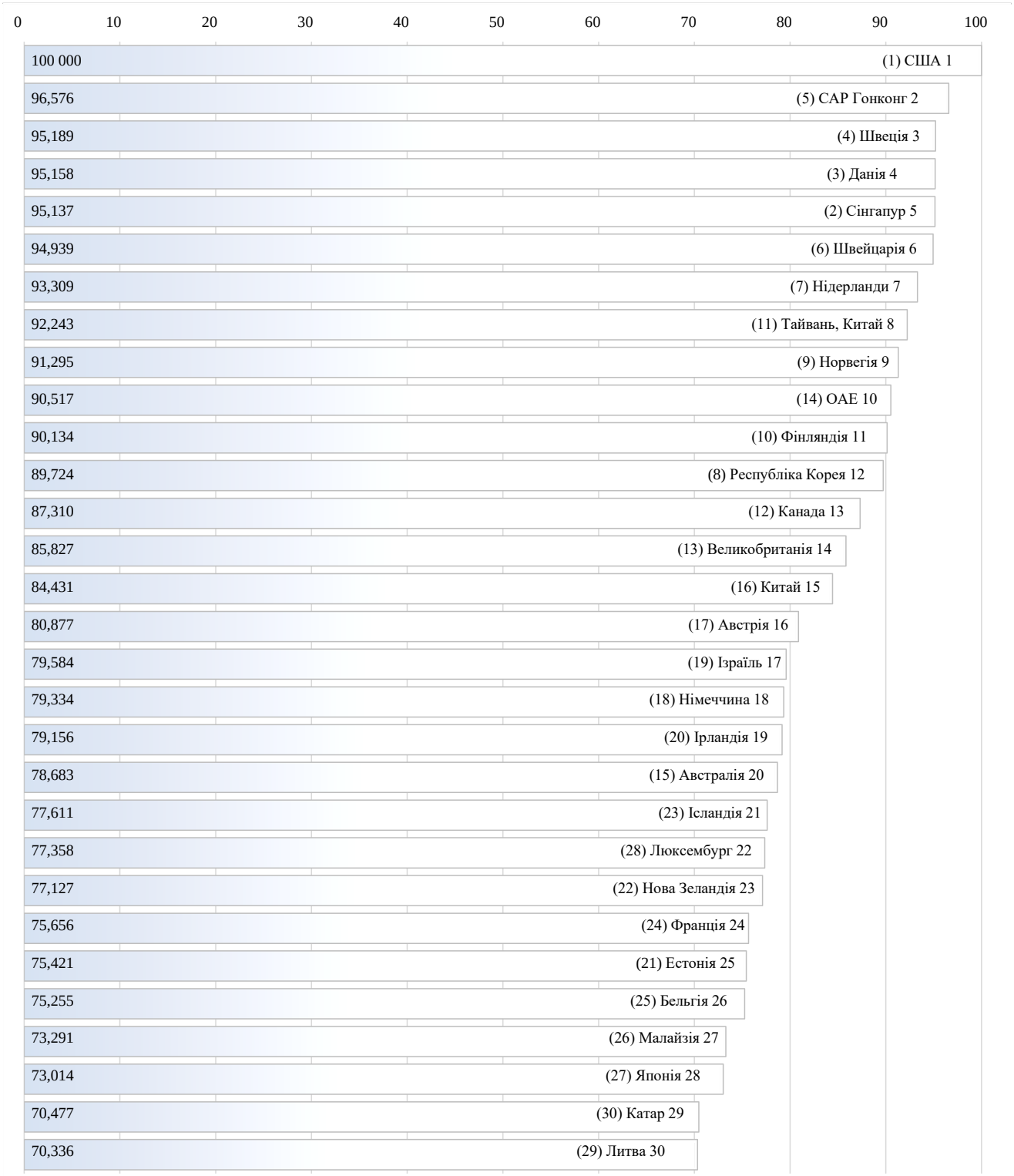
Рейтинг	Країна	Оцінка
1.	США	87
2.	Сінгапур	81
3.	Швейцарія	81
4.	Швеція	80
5.	Данія	77
6.	Фінляндія	76
7.	Нідерланди	75
8.	Великобританія	75
9.	Японія	75
10.	Норвегія	73
11.	Австралія	72
12.	Нова Зеландія	72
13.	Південна Корея	71
14.	Люксембург	70
15.	Німеччина	70
16.	Франція	70
17.	Канада	70
18.	Ірландія	69
19.	Бельгія	66
20.	Австрія	66
21.	ОАЕ	62
22.	Китай	62
23.	Іспанія	61
24.	Естонія	61
25.	Португалія	61
26.	Італія	60
27.	Литва	58
28.	Чехія	57
29.	Словенія	56
30.	Чилі	54
31.	Угорщина	54
32.	Словаччина	54
33.	Саудівська Аравія	53
34.	Малайзія	53
35.	Греція	52
36.	Болгарія	52
37.	Бахрейн	51
38.	Хорватія	51
39.	Польща	51

Рейтинг	Країна	Оцінка
40.	Уругвай	50
41.	Румунія	50
42.	Росія	50
43.	Оман	48
44.	Бразилія	47
45.	Казахстан	47
46.	Таїланд	46
47.	Білорусь	46
48.	Кувейт	46
49.	Туреччина	46
50.	Аргентина	45
51.	Сербія	45
52.	Україна	43
53.	Мексика	43
54.	Колумбія	42
55.	В'єтнам	41
56.	Південна Африка	41
57.	Перу	40
58.	Індонезія	39
59.	Філіппіни	38
60.	Марокко	38
61.	Еквадор	38
62.	Парагвай	37
63.	Індія	37
64.	Єгипет	36
65.	Венесуела	35
66.	Йорданія	35
67.	Ліван	32
68.	Болівія	32
69.	Алжир	32
70.	Кенія	31
71.	Ботсвана	31
72.	Гана	30
73.	Бангладеш	30
74.	Намібія	28
75.	Пакистан	28
76.	Нігерія	27
77.	Уганда	26
78.	Танзанія	25

Джерело: Global Connectivity Index 2020. https://www.huawei.com/minisite/gci/e

Додаток Г

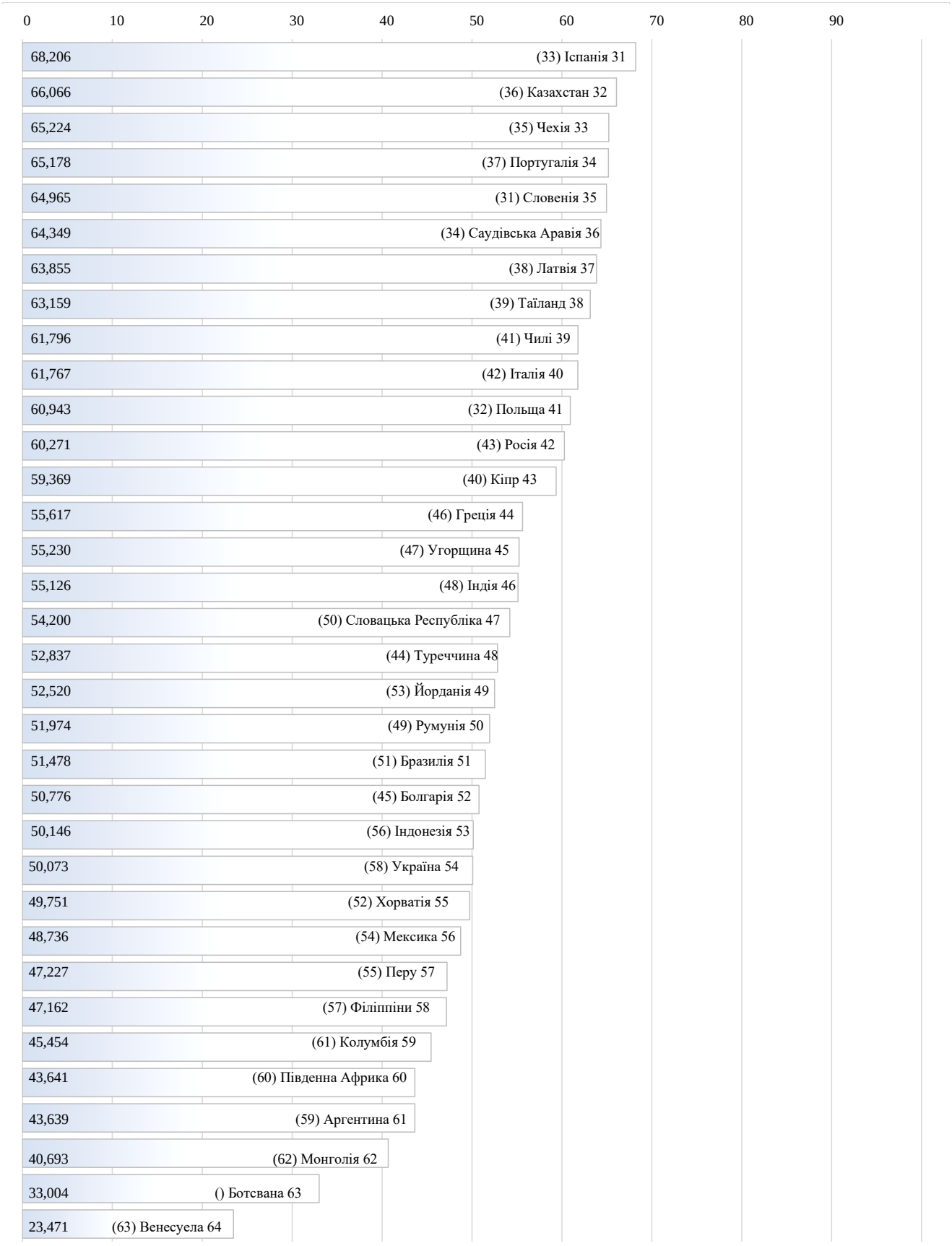
Глобальний рейтинг цифрової конкурентоспроможності країн у 2020 та 2021 рр.
(у дужках наводяться дані за 2020 рік)



Джерело: Світовий рейтинг конкурентоспроможності IMD. https://imd.cld.bz/Digital-Ranking-Report-2021/28/

-

РЕЙТИНГ ЦИФРОВОЇ КОНКУРЕНТОСПРОМОЖНОСТІ (31-64 ранги)



НАУКОВЕ ВИДАННЯ

Володимир Муравський

ОБЛІК ТА КІБЕРБЕЗПЕКА

Монографія

Підписано до друку – 11.11.2023 р.
Формат 60х84 1/16.
Гарнітура Times New Roman
Папір офсетний. Друк на дублікаторі.
Умов. друк. арк. 12,5
Тираж 100 прим.

Видавець та виготовлювач
Західноукраїнський національний університет
вул. Львівська, 11, м. Тернопіль 46004

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців ДК № 3467 від 23.04.2009 р.

МУКАЧІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

89600, м. Мукачево, вул. Ужгородська, 26
тел./факс +380-3131-21109
Веб-сайт університету: www.msu.edu.ua
E-mail: info@msu.edu.ua, pr@mail.msu.edu.ua
Веб-сайт Інституційного репозитарію Наукової бібліотеки МДУ: http://dspace.msu.edu.ua:8080
Веб-сайт Наукової бібліотеки МДУ: http://msu.edu.ua/library/