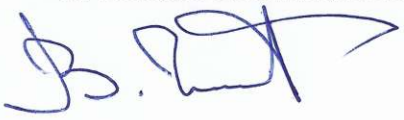
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ЧУБАЄВСЬКИЙ ВІТАЛІЙ ІВАНОВИЧ



УДК 330.131.5-049.65:[334.72:004.9

ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ СИСТЕМ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ

08.00.04 – економіка та управління підприємствами
(за видами економічної діяльності)

РЕФЕРАТ
дисертації на здобуття наукового ступеня
доктора економічних наук

Київ – 2023

Дисертацією є рукопис.

Робота виконана в Державному торговельно-економічному університеті Міністерства освіти і науки України, м. Київ

Офіційні опоненти:

доктор економічних наук, професор
ДЕЙНЕГА Олександр Вікторович,
проректор з наукової роботи Рівненського державного гуманітарного університету Міністерства освіти і науки України

доктор економічних наук, професор
МЕЛЬНИК Степан Іванович,
завідувач кафедри фінансів та обліку Львівського державного університету внутрішніх справ Міністерства внутрішніх справ України

доктор економічних наук, професор
ТАРАСЮК Галина Миколаївна,
декан факультету бізнесу та сфери обслуговування Державного університету «Житомирська політехніка» Міністерства освіти і науки України

Захист відбудеться 6 червня 2023 р. о 10:00 на засіданні спеціалізованої вченої ради Д 26.055.01 у Державному торговельно-економічному університеті за адресою: вул. Кіото, 23 (аудиторія Л-220), м. Київ, 02156.

З дисертацією можна ознайомитися в бібліотеці Державного торговельно-економічного університету за адресою: вул. Кіото, 19, м. Київ, 02156.

Вчений секретар
спеціалізованої вченої ради І.В. Федулова

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Основним трендом розвитку суспільства є інформатизація всіх сфер життя, в тому числі економічної сфери. На корпоративному рівні це призводить до зміни усталених підходів як до організації операційних процесів, так і технологій і інструментів управління. Водночас, змінюються погляди на визначальні чинники досягнення успіху та конкурентоспроможності на ринку: відбувається інтелектуалізація та гуманізація ресурсного потенціалу підприємства, де інформація стає важливим фактором виробництва. Розвиток інформаційних технологій з одного боку суттєво полегшує процес формування рішень та забезпечує їх принципово нову якість (за рахунок відкритості та доступності великих масивів даних, можливості формування та запровадження управлінських систем «у режимі реального часу», використання та швидкої обробки великих баз даних тощо), а з іншого – створює нові загрози та ризики для функціонування підприємства, рівень та інтенсивність виникнення яких постійно зростає.

За оцінками експертів станом на 2023 рік 70% людства буде користуватись Інтернетом. Це вагома ознака розвитку глобального інформаційного суспільства, що вимагає розробки та запровадження системних підходів кіберзахисту як на корпоративному, так і на державному рівнях. Практика останніх років засвідчує висхідний тренд вартості кіберзлочинів з одного боку, та низьку спроможність традиційних заходів кібербезпеки щодо їх стримування та запобігання. Актуальності набуває проблематика захисту інформації, протидії кібератакам, що потребує розробки нових рішень та підходів, які відповідають не тільки реаліям сьогодення, але й мають значний потенціал розвитку, ураховуючи сучасні загальні тенденції ІТ-галузі.

За даними державної служби статистики України, у 2021 році 86,6% підприємств України мали доступ до мережі Інтернет. Проте, на жаль, статистичні спостереження щодо запровадження підходів із забезпечення інформаційної безпеки підприємствами України на сьогодні відсутні. Водночас стан інформаційної безпеки України опосередковано демонструє її місце в Глобальному та Національному індексах кібербезпеки. Так, у 2018 році Україна посіла 54 місце серед 180 країн у Глобальному рейтингу кібербезпеки, посиливши свою позицію на 2 пункти, у 2020 році – 25 місце серед 160 країн у рейтингу Національного індексу кібербезпеки. Це свідчить про певне покращення систем захисту інформації в Україні, проте і вказує на наявний потенціал та необхідність запровадження заходів із посилення інформаційної безпеки.

Зазначені процеси та тенденції обумовили формування концепції інформаційної безпеки та виокремлення цілого напряму досліджень, присвячених обґрунтуванню методологічних засад та методичних підходів до її формування в економічних системах різного рівня – з одного боку, та розроблення програмних документів, нормативно-правових актів щодо її формування та розвитку інформаційного суспільства в цілому на національному та глобальному рівнях.

Проблематика захисту інформації, формування системи інформаційної безпеки досліджується в низці наукових праць закордонних та вітчизняних

фахівців. Аналіз значного масиву публікацій дозволив виокремити три принципові підходи до вивчення систем захисту інформації: 1) у складі вивчення теоретико-методологічних та практичних аспектів формування економічної безпеки, де інформаційна безпека розглядається як її важливий елемент; 2) як самостійний об'єкт дослідження з акцентом на управлінських, організаційних, правових аспектах формування системи інформаційної безпеки; 3) як самостійний об'єкт дослідження з переважним акцентом на технічних аспектах забезпечення інформаційної безпеки.

Так, в роботах Г.Менахем, В.Черілова, Б.Карайон, Ю.М. Харазішвілі, Е.В. Дронь, В.М. Геєця, М.О. Кизим, О.І. Черняк, З.С. Варналій, О.В. Панасюк, Я.А. Жаліло, В.В. Кузьменко, О.В. Арєф'євої, О. Бондаренко, В.А. Сухецького, Г.В. Козаченко, В.П. Пономарьова, О.М. Ляшенко, В.Л. Ортинського, І.С. Керницького, С.М. Шкарлет та ін. досліджуються методологічні засади формування системи економічної безпеки економічних систем різного рівня (держави, регіону, підприємства), виокремлюються її основні елементи, окреслюється методологія оцінювання, принципи формування систем забезпечення та напрями зміцнення. У зазначених роботах інформаційна безпека розглядається як складова більш складної системи, управління якою здійснюється в контексті та на загальних засадах керування економічною безпекою.

У дослідженнях Н. Муане, В.В. Андріанова, С.Л. Зефірова, В.Б. Голованова, А.А. Анісімова А.А., О.В. Герасименка, А.В. Козак, М.І. Глухова, О.О. Кузнецова, С.П. Євсеєва, П.Д. Біленчука, В. Панченка, Л.Г. Чистоклєтова, В.Ю. Світличної, Т.В. Полозової, М.Ю. Журавля, О.В. Стороженка, З.Б. Живка, А.О. Чередниченка, Л.В. Шмалія, О.О. Косиці, С.П. Міщенка, К.П. Боримської увага приділяється питанням регулювання, правового забезпечення інформаційної безпеки, формування організаційного механізму системи захисту інформації на підприємстві.

Технічним аспектам захисту інформації, а саме вдосконаленню графів атак для моніторингу кібербезпеки, оперуванню неточностями, обробці циклів, відображенню інцидентів і автоматичному вибору захисних заходів приділено увагу в роботах українських вчених: О.Г. Корченка, В.А. Савченка, Р.В. Грищука, О.К. Юдіна, О.В. Барабаш, І.С. Добриніна, Ю.Г. Даника, Ю.В. Копитіна, О.А. Смірнова, Г.В. Шукліна. Концептуальні моделі системи інформаційного впливу розробили В.А. Лужецький, А.В. Дудатьєв. Побудовою комплексних систем захисту складних інформаційних систем на основі структурного підходу та нейронних мереж займаються та займалися С.В. Тюлюпа, І.І. Пархоменко, Ю.І. Хлапонін, В.В. Козловський, А.В. Міщенко. Оцінювання захищеності інформаційних систем досліджували В.О. Хорошко, О.Г. Корченко, О.Г. Оксіюк, Ю.Є. Хохлачова, Н.В. Лукова-Чуйко, Ю.О. Ковтун, Б.Б. Ахметов, С.В. Казмірчук, Г.І. Гайдур, Є.А. Часновський.

Більшість дослідницьких зусиль іноземних вчених зосереджені на використанні мережевого трафіка для створення моделей прогнозування. Ці дослідження представлені в роботах таких вчених, як: Е. Понтес, А. Е. Гуельфі, С. Т. Кофуджі, А. А. Сільва. Інші дослідники, такі як, Д. Бансал, С. Софат, П. Чакраборті, П. Хадіві, Б. Льюіс, А. Махендиран, Дж. Чен, П. Батлер, Э. О. Нсозі, С.

Р. Мекару, Дж. С. Браунштейн, будують кіберпрогнозування за допомогою статистичного та алгоритмічного моделювання.

Не дивлячись на досить потужний пласт досліджень з проблематики інформаційної безпеки, на даний час відсутні комплексні міждисциплінарні розвідки, які б окреслювали методологію та практичний інструментарій формування ефективних систем захисту корпоративної інформації, які б забезпечували, з одного боку, дієвий захист інформації (убезпечували виток інформації, вихід з ладу комунікаційних засобів тощо), а з іншого – формували засади ефективного функціонування систем захисту інформації відповідно до економічних критеріїв ефективності. Зважаючи на те, що підприємство ринкової економіки завжди функціонує в умовах обмежених ресурсів на засадах самоокупності та самофінансування, саме відповідність критерію економічної ефективності систем захисту корпоративної інформації є важливою передумовою його розвитку. Відповідно, саме на обґрунтування теоретико-методологічних засад формування ефективних (з т. з. досягнення цілей захисту та цільових показників економічної ефективності) систем інформаційної безпеки спрямоване дане дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано відповідно до плану науково-дослідних робіт Державного торговельно-економічного університету. Результати досліджень наведено в темах: «Системи оцінювання економічної ефективності захисту корпоративної інформації» (термін виконання II кв. 2021 – III кв. 2024, номер державної реєстрації 0121U110908) запропоновано інтегральну методику оцінювання рівня ефективності системи захисту корпоративної інформації підприємства, яка передбачає розрахунок інтегральних показників за кожною виділеною складовою системи захисту корпоративної інформації підприємства й загального інтегрального показника; обґрунтовано шкалу інтерпретації рівня ефективності системи захисту корпоративної інформації підприємства за пропонованою методикою; розроблено підходи до математико-алгоритмічної та комп'ютерної підтримки процедури прийняття рішень у задачі організаційно-економічного забезпечення ефективного захисту корпоративної інформації; запропоновано методику багатокритеріальної оптимізації витрат на систему захисту корпоративної інформації, яка полягає в застосуванні генетичного алгоритму VEGA (Vector Evaluated Genetic Algorithm) (довідка № 1999/24 від 14.11.2022); «Цифрова трансформація торговельно-економічної та туристичної систем України» (№717/20; термін виконання 01.06.2022 – 31.12.2022; замовник – МОНУ; підстава для проведення НДР – наказ МОНУ від 16.04.2021 р. №434), де запропоновано методи оцінки економічної ефективності інформаційної безпеки для підприємств торгівлі; систематизовано особливості оцінки економічної ефективності інформаційної безпеки з урахуванням особливостей діяльності оптово-роздрібних підприємств; розроблено підходи до вирішення проблем захисту персональних даних в електронно-інформаційному середовищі торговельно-економічної та туристичної сфер України; запропоновано генетичний алгоритм розв'язання задачі масштабування хмароорієнтованого об'єкта

інформатизації в торговельно-економічній та туристичній сферах (довідка №2005/20 від 15.11.2022).

Мета та завдання дослідження. Метою дисертаційної роботи є комплексне наукове та практичне вирішення проблеми забезпечення економічної ефективності систем захисту корпоративної інформації.

Для досягнення поставленої мети визначено такі завдання:

проаналізувати соціально-економічний зміст, сутнісні характеристики поняття «корпоративний інформаційний простір», ідентифікувати основні етапи еволюції контенту корпоративної інформації та форм її організації;

дослідити та визначити місце та роль захисту корпоративної інформації в забезпеченні ефективного розвитку підприємства;

уточнити зміст поняття «ефективність захисту корпоративної інформації» на основі дослідження та розвитку видової трансформації економічної ефективності управління підприємством;

обґрунтувати Концепцію формування корпоративної інформаційної безпеки;

систематизувати види корпоративних політик інформаційної безпеки;

запропонувати систему показників оцінки економічної ефективності управління інформаційною безпекою та методологічний підхід до її оцінювання;

обґрунтувати комплекс ознак несанкціонованого доступу до корпоративної інформації;

розробити програмний комплекс для оцінки актуальності загроз витоку інформації;

сформувати модель оцінювання ефективності інвестицій на формування системи захисту корпоративної інформації;

здійснити порівняльну оцінку інформаційної безпеки в Україні та світі, виявити основні тенденції її формування;

провести аналіз діючої практики управління інформаційною безпекою на підприємствах;

оцінити економічну ефективність систем захисту корпоративної інформації в Україні;

розробити організаційно-економічне забезпечення ефективного захисту корпоративної інформації;

сформулювати методологічні засади та модель аудиту систем захисту безпеки корпоративної інформації;

визначити напрями вдосконалення оцінки ризиків інформаційної безпеки підприємства в автоматизованих системах захисту корпоративної інформації.

Об'єктом дослідження є процес забезпечення економічної ефективності систем захисту корпоративної інформації.

Предметом дослідження є теоретико-методологічні засади та практичні інструменти забезпечення економічної ефективності систем захисту корпоративної інформації.

Методи дослідження. Для вирішення поставлених у роботі завдань використані загальнонаукові й прикладні методи дослідження, взаємопов'язані та послідовно застосовані для забезпечення загальної логіки, зокрема, порівняльний, структурний та логіко-історичний (для дослідження сутності, еволюції та

особливостей корпоративного інформаційного простору, ролі захисту корпоративної інформації в забезпеченні розвитку підприємства, дослідженні видової трансформації економічної ефективності управління підприємством п.1.1, 1.2, 1.3.); системно-функціональний метод (для розроблення концепції формування системи корпоративної інформаційної безпеки, методологічних засад формування політики захисту корпоративної інформації, систематизації показників оцінювання економічної ефективності захисту корпоративної інформації п.2.1, 2.2, 2.3); методи системного аналізу, теоретичного узагальнення та синтетичних оцінок (для обґрунтування механізму формування корпоративної інформаційної безпеки, формування принципів оцінки та розроблення інтегрального показника економічної ефективності захисту корпоративної інформації п.2.1, 2.3); теорії ймовірності і математичної статистики (для оцінювання довірчих інтервалів математичного сподівання нормального розподілу випадкової величини інтенсивності кібератак (р. 3); методи порівняння, математичні та статистичні методи аналізу, анкетного опитування (для оцінки тенденцій зміни рівня інформаційної безпеки України, аналізу діючої практики захисту корпоративної інформації на підприємствах України та оцінки його ефективності р. 4); метод аналізу ієрархій (МАІ), метод нечітких правил, теорія Байєсовських мереж (БМ), елементи нечіткої логіки (НЛ), алгоритми штучних нейронні мережі (ШНМ) (для розроблення моделей оцінювання рівня безпеки корпоративної інформації (р. 5).

Інформаційною базою дисертаційної роботи є наукові праці вітчизняних та зарубіжних вчених, законодавчі акти Верховної Ради України, укази Президента України, постанови Кабінету Міністрів України, офіційні матеріали Державної служби статистики України, Євростату, офіційних інформаційних ресурсів міжнародних організацій, що регламентують питання інформаційної безпеки, матеріали міжнародних і регіональних науково-практичних конференцій, матеріали періодичних видань та електронні матеріали засобів масової інформації, результати соціально-економічних досліджень, результати анкетного опитування вибірки українських підприємств, результати власних досліджень.

Наукова новизна одержаних результатів дисертаційної роботи полягає в поглибленні теоретико-методологічних засад та наданні практичних рекомендацій, що спрямовані на розв’язання проблеми забезпечення ефективного захисту корпоративної інформації. Основними положеннями, розробленими автором особисто, що виносяться на захист, є такі:

вперше:

обґрунтовано авторську концепцію формування корпоративної інформаційної безпеки, що ґрунтується на позитивістській та нормативній економічних теоріях, поєднанні системного, процесного, проектного підходів в управлінні та концепції динамічних компетентностей, сформульованій системі принципів та механізмі забезпечення, що сприятиме більш комплексному розумінню проблем формування інформаційної безпеки та забезпеченню комплексності заходів щодо її забезпечення;

розроблено методологічний підхід до оцінювання ефективності захисту корпоративної інформації, який включає: принципи оцінювання та систематизації показників; систему часткових показників ефективності та критеріальну шкалу їх

інтерпретації; узагальнюючу оцінку ефективності захисту корпоративної інформації на основі поєднання інтегрального показника та показника прогресивності розвитку системи захисту корпоративної інформації (КІ), структурно-логічну послідовність етапів оцінювання, що створює основу для запровадження дієвих систем оцінювання ефективності захисту КІ;

запропоновано методологічний підхід до процедури опису ознакового функціонального подання неправомірних дій комп'ютерного зловмисника в ході реалізації функцій несанкціонованого доступу (НСД) до ресурсів інформаційної системи (ІС) підприємств за рахунок формалізації ієрархічної схеми формування множини ознак НСД до ресурсів ІС підприємства; отримана ієрархічна структура є основою для подальшого синтезу інтелектуальної системи виявлення спроб НСД в умовах важкозрозумілих ознак або їх невеликого числа, що дозволяє ефективно реалізувати первинну формалізацію неправомірних дій комп'ютерних зловмисників для подальшого математичного опису параметра ймовірності НСД;

сформована інтелектуальна система оцінки загроз витоку інформації щодо ТКПІ (технічних каналів передачі інформації) на основі методу аудиту інформаційної безпеки (АІБ), що грунтується на автоматизації процедур аудиту шляхом залучення для оцінки ризиків інформаційної безпеки апарату Байєсовських мереж (БМ) та штучних нейронних мереж (ШНМ). Дана система дозволяє підвищити ступінь достовірності результатів проведення комплексного аудиту інформаційної безпеки (ІБ) об'єктів інформатизації (ОБІ) та комплексної оцінки ризиків, своєчасно реагувати на загрози адміністратору ІБ розподіленої обчислювальної мережі (РОМ);

удосконалено:

визначення сутності корпоративного інформаційного простору шляхом виокремлення сутнісної ознаки «спосіб розвитку суб'єкта» та підхід до його структуризації шляхом виокремлення таких структурних компонентів: суб'єкт, семантична складова, інформаційна інфраструктура, регламенти та норми, що поглиблює розуміння його змісту та значення в забезпеченні корпоративного розвитку та формує теоретичне підґрунтя для розроблення методології та практичного інструментарію його захисту;

структуризацію етапів еволюції корпоративного інформаційного простору шляхом ідентифікації трьох етапів: «паперового», «автоматизованого», «мережевого» та виокремлення такої його особливості як посилений вплив на корпоративну структуру та бізнес-модель, що розширює уявлення про його функціонування та є основою для моделювання політики захисту КІП;

концептуальне позиціонування захисту корпоративної інформації в забезпеченні ефективного розвитку підприємства на основі доведеної взаємообумовлюючої залежності між параметрами та функціями корпоративного інформаційного простору (КІП); розширено перелік параметрів КІП такими характеристиками як рівень цифровізації КІП, цифрові компетентності персоналу, рівень інноваційності інформаційної інфраструктури, рівень корпоративної інформаційної культури, ступінь захищеності та якість регламентації КІП; ідентифіковано систему функцій КІП (інтегруюча, комунікативна, актуалізуюча, соціальна, навчальна, інноваційна, акселеруюча) та сформульоване авторське

бачення сутності захисту корпоративної інформації як системи принципів, методів та процесів протидії загрозам інформаційній безпеці підприємства, які спрямовуються на порушення функціонування КІП і передбачає їх ідентифікацію, аналіз, попередження та нейтралізацію, що поглиблює теоретичні основи функціонування КІП та формує підґрунтя для побудови систем управління ним;

теоретичний концепт сутності економічної ефективності управління підприємством на основі нової авторської трактовки змісту «управління підприємством» як інтегральної характеристики сукупності функціональних підрозділів, управлінських процесів, управлінських рішень, управлінського персоналу, центрів фінансової відповідальності в межах єдиного КІП та відповідно сформульованої її видової класифікації з визначеними сутністю та місцем у ній економічної ефективності захисту корпоративної інформації, що дозволило систематизувати основні методичні підходи до оцінювання ефективності захисту корпоративної інформації та сприятиме їх більш обґрунтованому вибору в практичній площині;

методологічний підхід до автоматизації та систематизації проявів ефекту захищеності інформації від витоків по технічних каналах шляхом доповнення імовірнісної моделі виконання загроз, який дозволяє на основі запропонованого програмного забезпечення (ПЗ) залучати кілька експертів для оцінки актуальності загроз витоку інформації щодо ТКПІ в умовах динамічного вдосконалення технічних засобів розвідки (ТЗР);

науковий підхід до організації процесу управління подіями інформаційної безпеки (ІБ) для підприємства, який на відміну від існуючих пропонує комплексну деталізацію алгоритму підпроцесу «Обробка подій» відповідно до життєвого циклу подій ІБ, що дозволить на практиці заповнити потенційні прогалини інформації при створенні системи управління ІБ підприємства, реалізовувати даний підпроцес у незалежному режимі, спростити процедуру управління ІБ підприємства в цілому та знизити витрати на її побудову для невеликих підприємств;

організаційно-економічне забезпечення ефективного захисту корпоративної інформації як комплексу взаємоузгоджених елементів (заходів) різної спрямованості та частоти застосування, які перебувають у постійній взаємодії, виступають частиною економічного механізму інформаційної безпеки, реалізуються на різних контурах управління та інтегровані в систему загальнокорпоративного управління для досягнення визначених цілей та який на відміну від існуючих передбачає чітку систематизацію елементів за їх функціональним напрямом, можливістю впливу на КІБ, частотою застосування, контуром управління. Це дозволило окреслити систематизований комплекс практичних заходів із захисту корпоративної інформації, що підвищить обґрунтованість та ефективність їх запровадження в практичній діяльності;

методичний підхід до моделювання системи оцінювання рівня інформаційної безпеки (ІБ) для об’єктів інформатизації (ОБІ), який на відміну від існуючих ґрунтується на методі аналізу ієрархій (МАІ) та дозволяє оцінювати її результативність за визначеними критеріями;

набули подальшого розвитку:

систематизація та узагальнення напрямів корпоративної політики інформаційної безпеки в частині обґрунтування домінантних чинників формування її базису в глобальному бізнес-середовищі з виокремленням таких, як: створення єдиного цифрового корпоративного бізнес-простору, зростання швидкості впровадження цифрових бізнес-стратегії з високим рівнем технологічного розгортання та інтенсивності порушень стійкості системи захисту корпоративної інформації, на основі чого, на відміну від превалюючих підходів, доведена необхідність підвищення ефективності корпоративної політики інформаційної безпеки за рахунок її гнучкого реагування на зміну стратегічних цілей діяльності корпоративних структур;

методичний підхід до оцінки економічної ефективності системи захисту корпоративної інформації, який, на відміну від наявних, передбачає здійснення оцінювання ступеня досягнення максимально можливого прибутку корпоративної структур за рахунок визначення потенційних можливостей системи захисту корпоративної інформації, який сприяє отриманню своєчасної та достовірної інформації як основи для прийняття та реалізації суб'єктами безпеки тактичних і стратегічних управлінських рішень та дозволяє надавати керівникам корпорацій комплексну оцінку ефективності управлінських дій щодо використання інноваційних технологій інформаційної безпеки на всіх ієрархічних рівнях організаційної структури управління;

наукові підходи до створення моделі, що описує процедуру формалізації завдання оптимізації системи захисту інформації (СЗІ) суб'єкта господарської діяльності (підприємства), яка на відміну від існуючих передбачає математико-алгоритмічну та комп'ютерну підтримку процедури прийняття рішень у питаннях організаційно-економічного забезпечення ефективного захисту корпоративної інформації в контексті завдань менеджменту інформаційної безпеки (ІБ) підприємств. Запропонований підхід дає можливість стороні захисту максимально ефективно визначати параметри організаційного управління інфраструктурою СЗІ підприємства;

адаптивний моніторинг інформаційної безпеки, який включає процедури оброблення та аналізу подій інформаційної безпеки в межах їх життєвого циклу, відповідає принципам ієрархічної пов'язаності, цілісності та подібності подій ІБ, і, на відміну від існуючих характеризується інваріантністю щодо способів реалізації інфраструктурних рішень ІБ підприємства та, зокрема, його КІС. Це дозволяє, не змінюючи методичний інструментарій, масштабувати даний підхід і адаптувати його до СУІБ різних підприємств;

методичний підхід до процедури аудиту інформаційної безпеки (АІБ), який на відміну від існуючих забезпечує багатостороннє оцінювання інформаційної безпеки об'єктів інформатизації на основі поєднання стандартних чисельних та експертних метрик оцінювання ІБ, що дозволяє оперативно в ході аудиту інформаційної безпеки (АІБ) визначати актуальні ризики ІБ ОБІ та автоматизувати процедури АІБ на основі застосування Байєсовських мереж (БМ) і штучної нейронної мережі (ШНМ), а адміністратору ІБ розподіленої обчислювальної мережі (РОМ) своєчасно та динамічно реагувати на загрози.

Практичне значення одержаних результатів дисертаційної роботи полягає в тому, що теоретичні і методологічні положення доведені до рівня конкретних методик і рекомендацій щодо підвищення економічної ефективності систем захисту корпоративної інформації, можуть бути використані в практичній діяльності підприємств у процесі реалізації систем захисту інформації, а також органами державної влади – під час реалізації державної політики, вдосконалення законодавчих, нормативно-правових актів, а саме: методика інтегрального показника стану корпоративного інформаційного простору для експрес-діагностування розвитку інформаційно-комунікаційних технологій у країні, інтегральна методика оцінювання рівня ефективності систем захисту корпоративної інформації підприємств зі шкалою інтерпретації рівня ефективності систем захисту корпоративної інформації підприємств (РНБО України, довідка від 01.11.2022); розширена схема адаптивного моніторингу інформаційної безпеки та метод аудиту інформаційної безпеки, заснований на автоматизації процедур із застосуванням для оцінки ризиків апарату Байєсовських мереж та штучних нейронних мереж (Департамент кіберполіції Національної поліції України, довідка № 9305/38/01-2022 від 26.10.2022); ієрархічна схема формування простору ознак несанкціонованого доступу до ресурсів інформаційної системи підприємства, методологічний підхід до автоматизації проявів ефекту захищеності інформації від витоків по технічних каналах та імовірнісна модель реалізації загроз, яка дозволяє на основі запропонованого програмного забезпечення у вигляді програмного комплексу «Assessment of threats» залучати кілька експертів для оцінки актуальності загроз витоку інформації щодо технічних каналів передачі інформації в умовах динамічного вдосконалення технічних засобів розвідки (Державної служби спеціального зв'язку та захисту інформації України, акт № 01-5479/ВС від 03.11.2022); методичний інструментарій математико-алгоритмічної і комп'ютерної підтримки процедури прийняття рішень у задачі організаційно-економічного забезпечення ефективного захисту корпоративної інформації (ТОВ «КАРМА ДІДЖИТАЛ ЛТД», довідка № 0111/1-2022 від 01.11.2022).

Положення, висновки та пропозиції дисертаційної роботи застосовано в освітньому процесі Державного торговельно-економічному університеті під час викладання дисциплін «Економічна безпека підприємства», «Економічна діагностика підприємства», «Архітектура та проєктування програмного забезпечення», «Хмарні та GRID технології», «Комп'ютерні мережі» та в навчально-методичному процесі під час підготовки навчального посібника, збірників тестових завдань, програм, робочих програм, опорних конспектів лекцій (довідка № 2000/22 від 14.11.2022).

Особистий внесок здобувача. Усі наукові результати, які одержані в дисертаційній роботі та виносяться на захист, здобуті автором особисто і відображені в наукових публікаціях. З наукових праць, опублікованих у співавторстві, у дисертації використано лише ті положення, ідеї та висновки, які є результатом самостійної роботи автора.

Апробація результатів дисертації. Основні положення і результати досліджень, викладені в дисертаційній роботі, доповідалися і отримали схвалення на 14 міжнародних і всеукраїнських науково-практичних конференціях та

наукових семінарах: XII Міжнародна науково-практична конференція «Сучасні проблеми економіки та бізнесу» (НАУ, м. Київ, 10–11 листопада 2022 р.), Міжнародна науково-практична конференція «Сучасні тренди соціально-економічних перетворень та інтелектуалізації суспільства в умовах сталого розвитку» (НУ «Запорізька політехніка», м. Запоріжжя, 10 листопада 2022 р.), 4th International Conference on Innovative Data Communication Technologies and Application (ICIDCA 2022) (м. Коїмбатур, Індія, 3–4 листопада 2022 р.), Міжнародна науково-практична конференція «Стратегічні орієнтири розвитку економіки, фінансів, обліку і права» (м. Полтава, 30 липня 2022 р.), 6th International Conference on Inventive Communication and Computational Technologies (ICICCT – 2022) (м. Тамілнад, Індія, 12–13 травня 2022 р.), 11th Computer Science On-line Conference 2022 (Чехія, 26–30 квітня 2022 р.), 4th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2022) (м. Тірунелвелі, Індія, 10–11 лютого 2022 р.), International Conference on Computational Intelligence and Data Analytics (ICCIDA – 2022) (м. Гайдарабад, Індія, 8–9 січня 2022 р.), X Міжнародна науково-практична конференція «Інформаційно-аналітичне забезпечення управління фінансово-економічною безпекою держави, регіону, суб'єктів господарювання в умовах COVID-19» (ХНУМГ ім. О. М. Бекетова, м. Харків, 18–19 листопада 2021 р.), II Міжнародна науково-практична конференція «Глобалізаційні виклики розвитку національних економік» (КНТЕУ, м. Київ, 19 жовтня 2021 р.), 5th Computational Methods in Systems and Software 2021 (Чехія, 13–15 жовтня 2021 р.), IX Міжнародна науково-практична Інтернет-конференція «Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2021» (НУБіП України, м. Київ, 13–14 травня 2021 р.), IV Міжнародна науково-практична конференція проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS) (Київський національний університет імені Тараса Шевченка, м. Київ, 15–16 квітня 2021 р.), Наукові семінари «Кібергігієна. Кібербезпека. Безпека держави» (КНТЕУ, м. Київ, 27 листопада 2020 р.).

Публікації. Основні положення та результати дисертації опубліковано в 37 наукових працях, у т. ч.: одній одноосібній монографії; 23 наукових статтях, які надруковано в наукових фахових виданнях України та в наукових періодичних виданнях інших держав та виданнях України, які включені до міжнародних наукометричних баз (з них 8 статей у виданнях, проіндексованих у базах даних «Scopus» і «Web of Sciens Core Collection»), 13 працях апробаційного характеру (з них 5 праць, проіндексовані у базі даних «Scopus»). Загальний обсяг опублікованих наукових праць становить 39,1 друк. арк., з них автору належить 23,7 друк. арк.

Структура й обсяг дисертації. Дисертація складається з анотації, вступу, п'яти розділів основної частини зі списками використаних джерел до кожного з них, висновків та додатків. Повний обсяг дисертації становить 371 сторінка, з них основна частина займає 300 сторінок. Дисертація містить 34 таблиці та 36 рисунків, списки використаних джерел включать загалом 440 найменувань.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЇ

У вступі обґрунтовано актуальність теми дисертації, визначено зв'язок роботи з науковими темами, сформульовано мету, завдання, об'єкт, предмет і методи дослідження, розкрито наукову новизну та практичне значення отриманих результатів, наведено дані щодо апробації результатів дисертаційної роботи та їх опублікування.

У першому розділі «Теоретичні основи дослідження економічної ефективності систем захисту корпоративної інформації» досліджено еволюцію контенту та форми організації корпоративного інформаційного простору, розглянуто захист корпоративної інформації як детермінанту ефективного розвитку підприємства, а також видову трансформацію економічної ефективності управління підприємством.

Надано авторське визначення поняття «корпоративний інформаційний простір» – організована система інформації та інформаційних процесів корпорації, яка є станом та результатом її функціонування, способом її розвитку та представлення. Виокремлено три принципові етапи процесу еволюції корпоративного інформаційного простору: «паперовий», «автоматизований» і «мережевий». Останній етап, що триває по теперішній час, характеризується глобальним характером, високим рівнем інтенсивності та швидкості поширення інформації, її «надлишковим» характером, зниженням витрат часу на обробку та аналіз інформації, зростанням витрат на убезпечення інформаційного простору, суттєвим впливом на трансформацію бізнес-моделі, організаційної структури підприємства, способу виробництва товарів та послуг.

Виокремлено чотири принципові компоненти в межах складної структури корпоративного інформаційного простору: суб'єкти, семантичну складову (інформаційний контент), інформаційну інфраструктуру, регламенти та норми. Центральним та системоутворюючим компонентом корпоративного інформаційного простору є його суб'єкти, серед яких варто виокремити первинний та вторинний рівні. Первинними суб'єктами є персонал корпорації, здебільшого управлінський, який активно працює з інформацією. Вторинним суб'єктом є сама корпорація, яка є єдиним суб'єктом у зовнішньому по відношенню до неї просторі. Наступним компонентом є семантична складова, тобто сам інформаційний контент, який запропоновано умовно поділяти на: інформаційні поля; інформаційний процес; віртуальну реальність; інформаційну культуру.

З'ясовано роль та місце захисту корпоративної інформації в процесі формування інформаційної безпеки та економічної ефективності функціонування підприємства в умовах цифровізації та зростаючої ролі інформації. Установлено, що збільшення ризиків втрати інформації потребує формування корпоративної інформаційної безпеки – стану захищеності інтересів підприємства від недобросовісних дій (умисних та неумисних) щодо корпоративної інформації, що спрямовані на всі компоненти корпоративного інформаційного простору.

Визначено важливі параметри корпоративного інформаційного простору, до яких належать: інтенсивність інформаційного обміну, насиченість інформаційних полів, рівень цифровізації, цифрова компетентність персоналу, рівень

корпоративної інформаційної культури, рівень інноваційності корпоративного інформаційного простору, його захищеність та якість регламентації. Установлено, що від зазначених параметрів залежить здатність корпоративного інформаційного простору забезпечувати якісне виконання таких функцій: інтегруючої, комунікативної, актуалізуючої, соціальної, навчальної, інноваційної та акселеруючої. У свою чергу, від виконання корпоративним інформаційним простором своїх функцій на якісно високому рівні залежать результати діяльності підприємств за рахунок більш ефективного використання всіх видів ресурсів.

Узагальнено та систематизовано класифікацію загроз інформаційній безпеці підприємства та визначено зміст поняття «захист корпоративної інформації» як систему принципів, методів та процесів протидії загрозам інформаційній безпеці підприємства, спрямованих на порушення функціонування корпоративного інформаційного поля, і передбачає ідентифікацію, аналіз, попередження та нейтралізацію цих загроз. Представлено **концепт-модель місця захисту корпоративної інформації в забезпеченні ефективного функціонування підприємства** (рис. 1), відповідно до якої захист корпоративної інформації пов'язаний із захистом корпоративного інформаційного поля від різноманітних загроз з метою збереження високої якості його параметрів та забезпечення можливості ефективно виконувати свої функції.

На основі аналізу, узагальнення та систематизації сучасних підходів до тлумачення змісту економічної ефективності розмежовано поняття «економічна ефективність функціонування підприємства», «економічна ефективність управління підприємством» та розглянуто видову трансформацію останньої. Ураховуючи систематизацію основних характеристик поняття «управління», підходів до його організації з позицій системного підходу, визначено економічну ефективність управління підприємством як інтегровану характеристику ефективності (міри отриманого ефекту до ресурсів або понесених витрат) функціонування всіх його підсистем: функціональних підрозділів, центрів відповідальності, процесів, управлінських рішень, управлінського персоналу, яка суттєво детермінує ефективність функціонування підприємства. Відповідно представлено деталізовану класифікацію видів економічної ефективності управління підприємством, у межах якої чільне місце посідає економічна ефективність захисту корпоративної інформації – міра економічного ефекту витрачених ресурсів на реалізацію системи заходів з ідентифікації, аналізу, попередження та нейтралізації загроз порушення функціонування корпоративного інформаційного простору.

Ідентифіковано та систематизовано основні методичні підходи, які можуть бути покладені в основу оцінки економічної ефективності захисту корпоративної інформації, що зводиться до необхідності визначення витрат на здійснення такого захисту та економічного ефекту, що забезпечує цей захист.

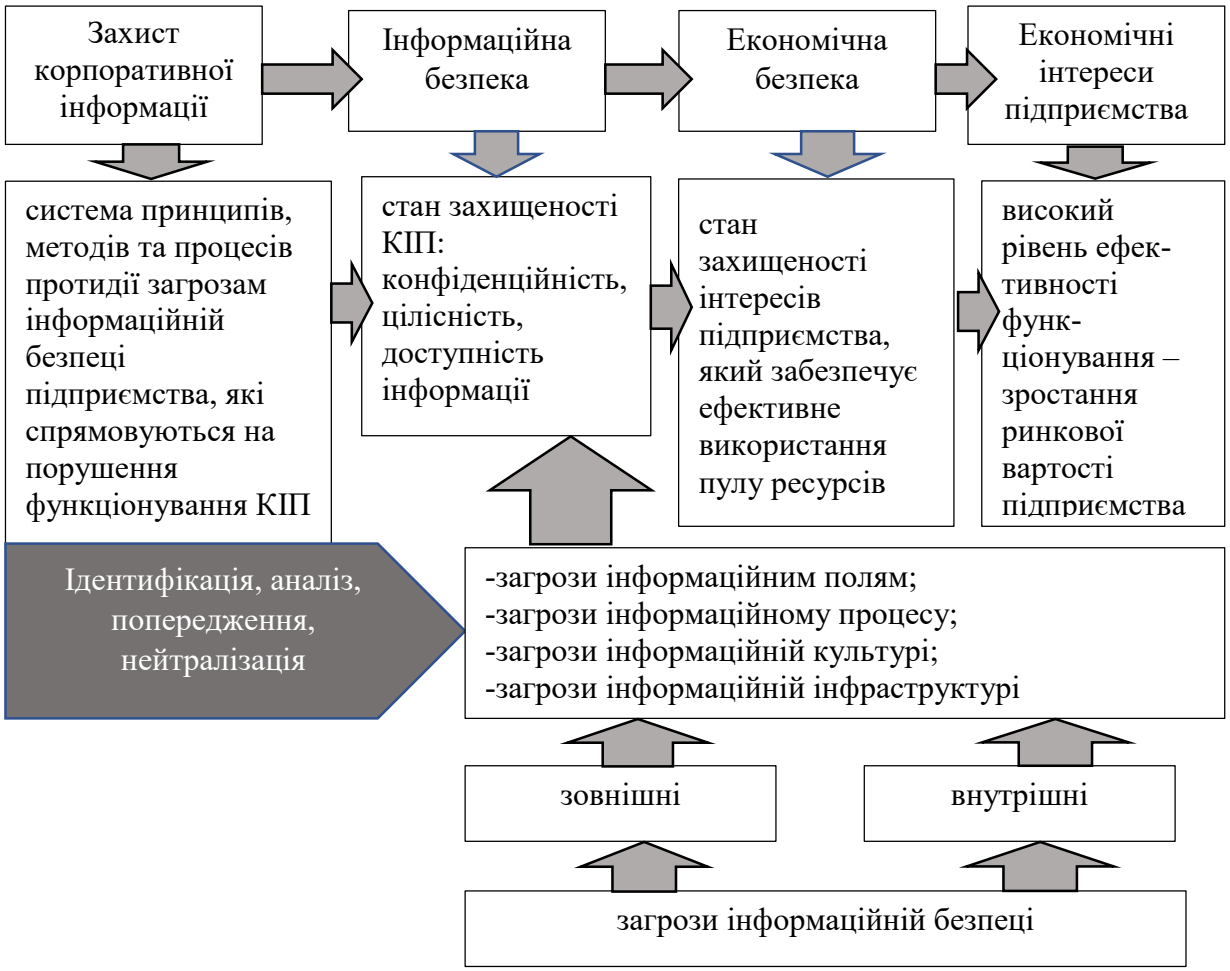


Рис. 1. Концепт-модель місця захисту корпоративної інформації в забезпеченні ефективного функціонування підприємства

Джерело: складено автором

У другому розділі «Методологічні основи управління корпоративною інформаційною безпекою» обґрунтовано концепцію формування корпоративної інформаційної безпеки, розроблено методологічні засади формування корпоративної політики інформаційної безпеки, систематизовано показники оцінки економічної ефективності управління корпоративною інформаційною безпекою.

На основі аналізу, синтезу та розвитку сучасних підходів до розуміння сутності концепції визначено зміст концепції формування корпоративної інформаційної безпеки як систему поглядів на організацію та забезпечення такої безпеки, що відображається через обрану методологію формування, окреслені принципи та розроблений механізм забезпечення. Відповідно до запропонованого визначення концепція формування корпоративної інформаційної безпеки містить три принципові структурні компоненти: методологічну основу, принципи та механізм. Зазначені структурні компоненти знаходяться в логічному зв'язку та підпорядкуванні.

Виокремлено два підрівні методологічної бази – структурної компоненти корпоративної інформаційної безпеки – «метаметодологію» та «підходи до управління». В основу метаметодології, що визначає загальні філософські основи

пізнання світу та окремих явищ та процесів, з наявних загальнонаукових та філософських концепцій пізнання світу в основу формування підходів до забезпечення інформаційної безпеки запропоновано покласти методологію позитивізму та нормативну теорію. Інший підрівень методології – підходи до управління – спрямований на конкретизацію метаметодології і окреслює підходи до управління корпоративною інформаційною безпекою, що покладаються в основу вибору засобів впливу на об'єкт управління, оцінювання тощо. Відповідно до сучасних умов господарювання та розвитку теорії менеджменту запропоновано покласти в основу побудови системи забезпечення корпоративної інформаційної безпеки, інтеграцію системного, процесного, проєктного підходів та концепції динамічних здатностей.

Виокремлено принципи корпоративної інформаційної безпеки: законності, дотримання балансу інтересів, системності, плановості, комплексності, безперервності, взаємної відповідальності, розумної достатності, персональної мінімізації повноважень, обов'язковості контролю, превентивного характеру заходів інформаційної безпеки, креативності та інноваційності, економічної ефективності, ситуативності та адаптивності, ризик-орієнтованості.

Досліджено механізм корпоративної інформаційної безпеки, який є сукупністю об'єктів, суб'єктів, мети, завдань, функцій та методів впливу. Останні систематизовані за окремими видами: економічні, організаційно-правові, технічні. Представлений перелік методів впливу на стан інформаційної безпеки, з одного боку, є далеко невичерпним, а з іншого – достатньо варіативним. Підприємство обирає методи управління інформаційною безпекою залежно від особливостей внутрішнього і зовнішнього середовища, обраної стратегії захисту тощо.

Узагальнені та систематизовані напрями корпоративної політики інформаційної безпеки, які характеризуються багатовимірністю, системністю, можливістю врахування та аналізу домінантних чинників формування її базису, що дає змогу врахувати стратегічну і тактичну складові корпоративної політики інформаційної безпеки, визначити елементи її конфігурації, які забезпечать можливість залучення суб'єктів різних рівнів з метою вчасного виявлення, попередження та ліквідації наслідків впливу дестабілізуючих чинників для досягнення інтересів корпоративних структур. Здійснено аналіз процесу управління корпоративною інформаційною безпекою, виявлено його надзвичайну складність з декількох причин: по-перше, підприємства функціонують в умовах постійно зростаючих загроз (як кількості, так і ступеня агресивності), що потребує постійного вдосконалення системи управління, креативності, інноваційності та випереджального характеру заходів; по-друге, реалізація заходів з протидії інформаційним загрозам завжди обмежується ресурсним потенціалом підприємства, перед усім – наявним бюджетом.

Установлено наявність методологічних перешкод у процесі вимірювання економічної ефективності управління корпоративною інформаційною безпекою: отриманий дохід, або прибуток, що оцінюється як непонесений (відвернений) збиток, завжди є складно і неточно детермінованим показником; витрати на забезпечення інформаційної безпеки носять різнорідний характер та з точки зору бухгалтерського обліку відносяться до різних періодів; окремий ефект у захисті

корпоративної інформації може досягатися за рахунок еволюційних змін процесів, які не носять дуже витратного характеру, але сам ефект від таких вдосконалень складно виокремити (до того ж він не знаходить відображення в окремих документах бухгалтерського обліку та звітності підприємства, що потребує специфічних налаштувань у системі збору інформації та введення додаткових звітів у системі управлінського обліку). Поставлено під сумнів можливість розроблення та застосування єдиної методики для формування вичерпного висновку щодо ефективності корпоративної інформаційної безпеки, натомість обґрунтовано необхідність уніфікації: принципів оцінювання, підходів до систематизації показників економічної ефективності, критеріїв оцінювання, логічної послідовності процедури оцінювання та формування інтегрального показника ефективності.

Сформульовано принципи оцінювання ефективності захисту корпоративної інформації: помірної деталізації, орієнтації на контур управління, ієрархічності, комбінації методів аналізу, логічної структурованості етапів оцінки. На основі зазначених принципів систематизовано та доповнено показники оцінювання ефективності захисту корпоративної інформації за контурами управління, методом виміру, рівнем ієрархії, рівнем узагальнення результатів оцінки, сформульовано підхід до оцінювання інтегрального показника ефективності захисту корпоративної інформації та логічну послідовність етапів її оцінювання. Це дозволить структурувати процес оцінки ефективності захисту корпоративної інформації.

У третьому розділі «Моделі та технології захисту корпоративної інформації» систематизовано ознаки несанкціонованого доступу до корпоративної інформації, розроблено програмний комплекс для оцінки актуальності загроз витоку інформації, здійснено моделювання ефективності інвестицій на формування системи захисту корпоративної інформації.

Запропоновано підхід до процедури формалізації ознакового функціонального подання неправомірних дій комп’ютерного зловмисника в ході реалізації функцій несанкціонованого доступу до ресурсів інформаційних систем підприємств.

Виконано формалізацію ієрархічної схеми формування простору ознак несанкціонованого доступу до ресурсів інформаційної системи (ІС) підприємства, фрагмент якої ілюструє табл. 1.

Отримана ієрархічна структура є основою для подальшого синтезу інтелектуальної системи виявлення спроб несанкціонованого доступу в умовах важкозрозумілих ознак або їх невеликого числа. Це дозволяє ефективно реалізувати первинну формалізацію неправомірних дій комп’ютерних зловмисників для подальшого математичного опису параметра ймовірності несанкціонованого доступу, наприклад, на основі Марківських ланцюгів. Конкретизація багатофакторного характеру реалізацій функцій несанкціонованого доступу до інформаційних ресурсів інформаційних систем заснована на Марківському ланцюзі. Розглянуто варіант, у якому представлення ознак несанкціонованого доступу виходить з побудови комбінаційної функціональної моделі неправомірних дій порушника інформаційної безпеки.

Запропоновано методологічний підхід, що дозволяє автоматизувати та систематизувати прояви ефекту захищеності інформації від витоків по технічних каналах. Доповнено імовірнісну модель виконання загроз, яка дозволяє на основі запропонованого програмного забезпечення (ПЗ) у вигляді програмного комплексу «Assessment of threats» залучати кілька експертів для оцінки актуальності загроз витоку інформації щодо технічних каналів передачі інформації в умовах динамічного вдосконалення технічних засобів розвідки (рис. 2).

Таблиця 1

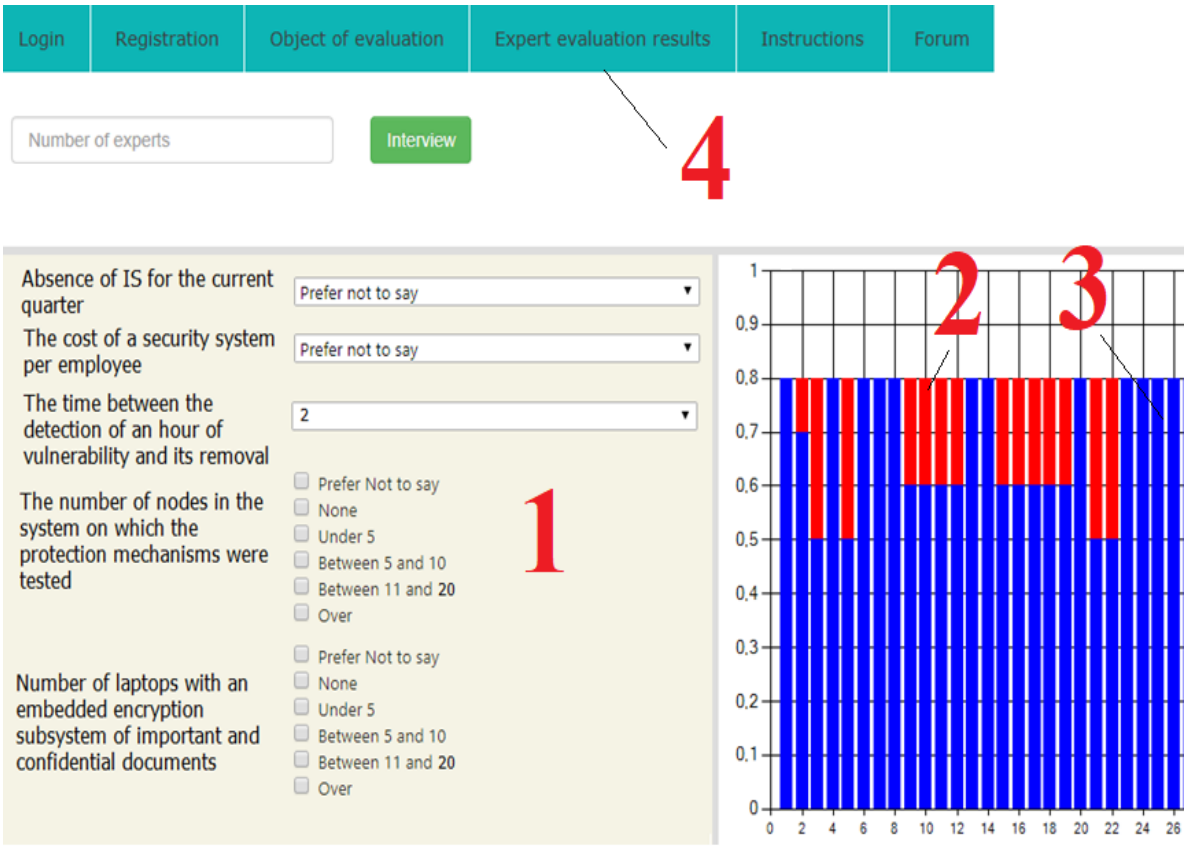
Фрагмент формалізації ієрархічної схеми формування простору ознак несанкціонованого доступу до ресурсів ІС підприємства

<table>
<tr><td rowspan="3">№з/п</td><td colspan="4">Ієрархічні рівні</td></tr>
<tr><td colspan="2">Перший</td><td colspan="2">Другий</td></tr>
<tr><td>Найменування</td><td>Позначення</td><td>Найменування</td><td>Позначення</td></tr>
<tr><td colspan="5">Функції збору відомостей про</td></tr>
<tr><td>1</td><td>ІС підприємства, об’єкта атаки</td><td>$c_1^{(1)}$</td><td>…</td><td>$c_1^{(2)}$</td></tr>
<tr><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td></tr>
<tr><td colspan="5">Знімання інформації з</td></tr>
<tr><td>7</td><td>клавіатур ПК</td><td>$c_7^{(1)}$</td><td rowspan="3">Установлення закладного ПЗ</td><td rowspan="3">$c_7^{(2)}$</td></tr>
<tr><td>8</td><td>моніторів ПК</td><td>$c_8^{(1)}$</td></tr>
<tr><td>9</td><td>мережевих пристроїв ІС та ін.</td><td>$c_9^{(1)}$</td></tr>
<tr><td colspan="5">Упровадження в ІС підприємства шкідливого програмного забезпечення (ПЗ)</td></tr>
<tr><td>10</td><td>мережевих черв’яків</td><td>$c_{10}^{(1)}$</td><td rowspan="3">Упровадження шкідливого ПЗ (наприклад, черв’яки: поштові (Mail-Worm); P2P (P2P-Worm); в IRC-каналах (IRC-Worm); мережеві (Net-Worm) та ін. Аналогічно для троянського ПЗ та ПЗ, яке використовує вразливості ОС та/або ІС</td><td rowspan="3">$c_{10}^{(2)}$</td></tr>
<tr><td>11</td><td>троянського ПЗ</td><td>$c_{11}^{(1)}$</td></tr>
<tr><td>12</td><td>ПЗ, яке використовує вразливості ОС та/або ІС</td><td>$c_{12}^{(1)}$</td></tr>
<tr><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td></tr>
</table>

Джерело: розроблено автором

Розроблене ПЗ у комплексі з програмним забезпеченням, яке призначене для оцінки ризиків втрати інформації, дозволяє комплексно оцінити рівень захищеності технічних каналів передачі інформації підприємства. Розроблене ПЗ сприяє зниженню витрат на проведення вузькоспеціальних досліджень у питаннях щодо оцінки актуальності загроз витоку інформації з технічних каналів передачі інформації в умовах динамічного вдосконалення технічних засобів розвідки. Таким чином, було досягнуто основної мети даного розділу дисертації – автоматизувати процедуру оцінки актуальності загроз витоку інформації з технічних каналів передачі інформації в умовах динамічного вдосконалення технічних засобів розвідки та вдосконалити процес оцінювання захищеності приміщень підприємств шляхом використання релевантних оцінок експертів.

Запропоновано методику розрахунку показників ефективності інвестиційних заходів у рамках підвищення метрик інформаційної безпеки об'єкта інформатизації. Описано конкретний приклад імітаційного моделювання. У запропонованій методиці передбачено оцінку попереджених збитків від кібератаки. Як базисний показник розрахунку економічного ефекту від інвестування в системи захисту інформації прийнято розмір попередженого збитку від кібератаки.



Умовні позначення: 1 – анкета експерта; 2 – актуальні загрози витоку інформації через технічні канали передачі інформації (червоні стовпці); 3 – нормативний рівень захисту технічних каналів передачі інформації від витоків досягнуто (сині стовпці); 4 – головне меню програмного комплексу «Assessment of threats»

Рис. 2. Загальний вигляд програмного комплексу «Assessment of threats» для оцінки актуальності загроз витоку інформації

Джерело: складено автором

Проведено імітаційне моделювання для конкретного прикладу розрахунку ефективності інвестування в інформаційну безпеку об'єкта інформатизації. Це дозволило врахувати відносну невизначеність реальної ситуації з інформаційною безпекою об'єкта інформатизації. Показано, що проведені дослідження допоможуть практикам у сфері інформаційної безпеки отримувати з допомогою викладеного в роботі підходу обґрунтовані рішення підвищення ефективності інвестиційних проектів у сфері інформаційної безпеки для об'єктів інформатизації. На відміну від існуючих, у запропонованій методиці враховані як прямі, так і непрямі чинники інвестиційних проектів у сфері інформаційної безпеки об'єкта інформатизації.

У четвертому розділі «Економічна діагностика систем захисту корпоративної інформації» проаналізовано діючу практику управління інформаційною безпекою (ІБ) на підприємствах та оцінено економічну ефективність системи захисту корпоративної інформації.

Визначено, що в процесі алгоритмізації процедур, пов'язаних з обробкою та аналізом подій ІБ у межах їх життєвого циклу, та відповідно до принципу цілісності об'єкти захисту (зокрема, корпоративні інформаційні системи) слід аналізувати в різних ракурсах. Такий аналіз починається з окремих компонентів об'єкта захисту та закінчується його аналізом загалом, у тому числі аналізом зовнішнього середовища. Реалізація принципів цілісності та подібності подій ІБ у ході управління адаптивними параметрами процедур моніторингу та обробка та подій ІБ у рамках їх життєвого циклу полягає в побудові взаємних відображень між завданнями ІБ та відповідними методами їх вирішення. Керуючись подібними відображеннями, можна оптимізувати схеми моніторингу, сконцентрувавши увагу на ієрархічній пов'язаності подій ІБ. Така ієрархічна пов'язаність дозволяє отримати біоактивне відображення ІБ об'єкта захисту, маючи необхідні дані моніторингу подій ІБ. Запропонована схема адаптивного моніторингу ІБ, включаючи процедури обробки та аналізу подій ІБ у межах їх життєвого циклу, відповідає принципам ієрархічної пов'язаності, цілісності та подібності подій ІБ.

Запропоновано доповнення до способу організації процесом управління подіями ІБ для корпоративної інформаційної системи (КІС) підприємства (рис. 3).

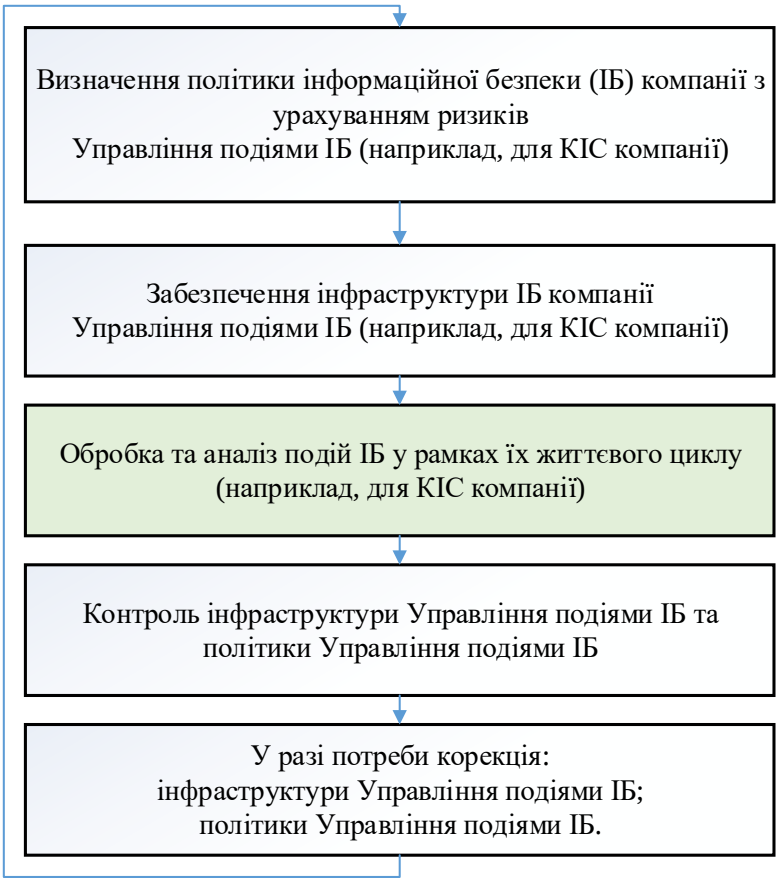


Рис. 3. Схема адаптивного процесу Управління подіями ІБ компанії (підприємства)

Джерело: складено автором

На відміну від існуючих рішень, деталізовано алгоритм підпроцесу «Обробка подій». Деталізація охоплює життєвий цикл події ІБ (рис. 4).

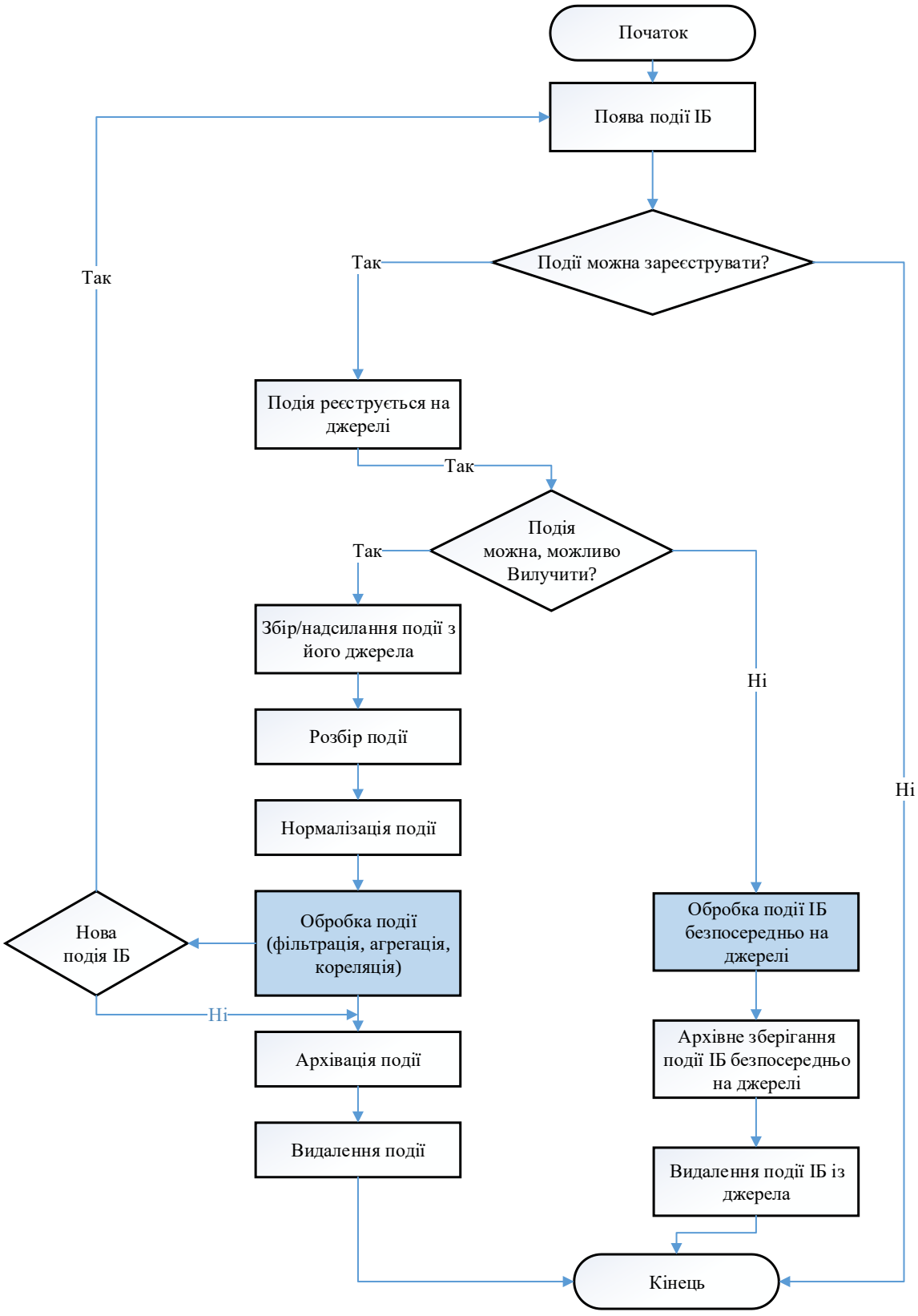


Рис. 4. Обробка та аналіз подій ІБ у рамках їх життєвого циклу

Джерело: складено автором

Виконані дослідження дозволяють на практиці заповнити потенційні прогалини інформації при створенні системи управління інформаційної безпеки підприємства, спростити процедуру управління загалом і знизити витрати на її побудову для невеликих підприємств.

Доповнено схему адаптивного моніторингу інформаційної безпеки, яка включає процедури оброблення та аналізу подій інформаційної безпеки в межах їх життєвого циклу (рис. 5).

Запропонована схема відповідає принципам ієрархічної пов'язаності, цілісності та подібності подій інформаційної безпеки. Запропоновані рішення та доповнення на відміну від аналогічних досліджень характеризуються інваріантністю щодо способів реалізації інфраструктурних рішень інформаційної безпеки підприємства та, зокрема, його корпоративної інформаційної системи. Це, зрештою, дозволяє, не змінюючи методичний інструментарій, масштабувати даний підхід і адаптувати його для систем управління інформаційною безпекою різних підприємств.

Оцінювання економічної ефективності системи захисту корпоративної інформації дозволило визначити ступінь досягнення максимально можливого прибутку корпоративними структурами та розробити рейтингову шкалу оцінки ефективності системи захисту корпоративної інформації, посилити управлінські заходи в процесі формування стратегії та механізмів забезпечення комплексної системи корпоративної інформаційної безпеки при формування адекватних заходів, спрямованих на виявлення та усунення проблем функціонування системи захисту корпоративної інформації, зменшення негативного впливу викликів і загроз інформаційної безпеці, попередження або мінімізацію можливих збитків.

У п'ятому розділі «Методи підвищення економічної ефективності захисту корпоративної інформації» досліджено організаційно-економічне забезпечення ефективного захисту корпоративної інформації, обґрунтовано теоретико-методичні засади аудиту інформаційної безпеки підприємства, удосконалено підходи до оцінювання ризиків інформаційної безпеки підприємства в автоматизованих системах захисту корпоративної інформації.

Визначено, що створення організаційно-економічного забезпечення захисту корпоративної інформації є необхідним елементом досягнення ефективності цього процесу, а набір елементів такого забезпечення диференціюється залежно від розміру, структури, рівня цифровізації процесів підприємства. Запропоновано типологію підприємств, що визначає вибір організаційно-економічних заходів захисту корпоративної інформації і базується на комбінації двох принципово важливих змінних «розмір підприємства – рівень його цифровізації» (рис. 6).

Доповнено методику оцінювання ефективності інвестиційних заходів у рамках підвищення метрик ІБ підприємства (ОБІ). На відміну від існуючих рішень, у запропонованій методиці передбачено оцінку попередженої шкоди від кібератаки. Як базовий показник розрахунку економічного ефекту від інвестування в засоби захисту інформації прийнято розмір попередженого збитку від кібератаки.

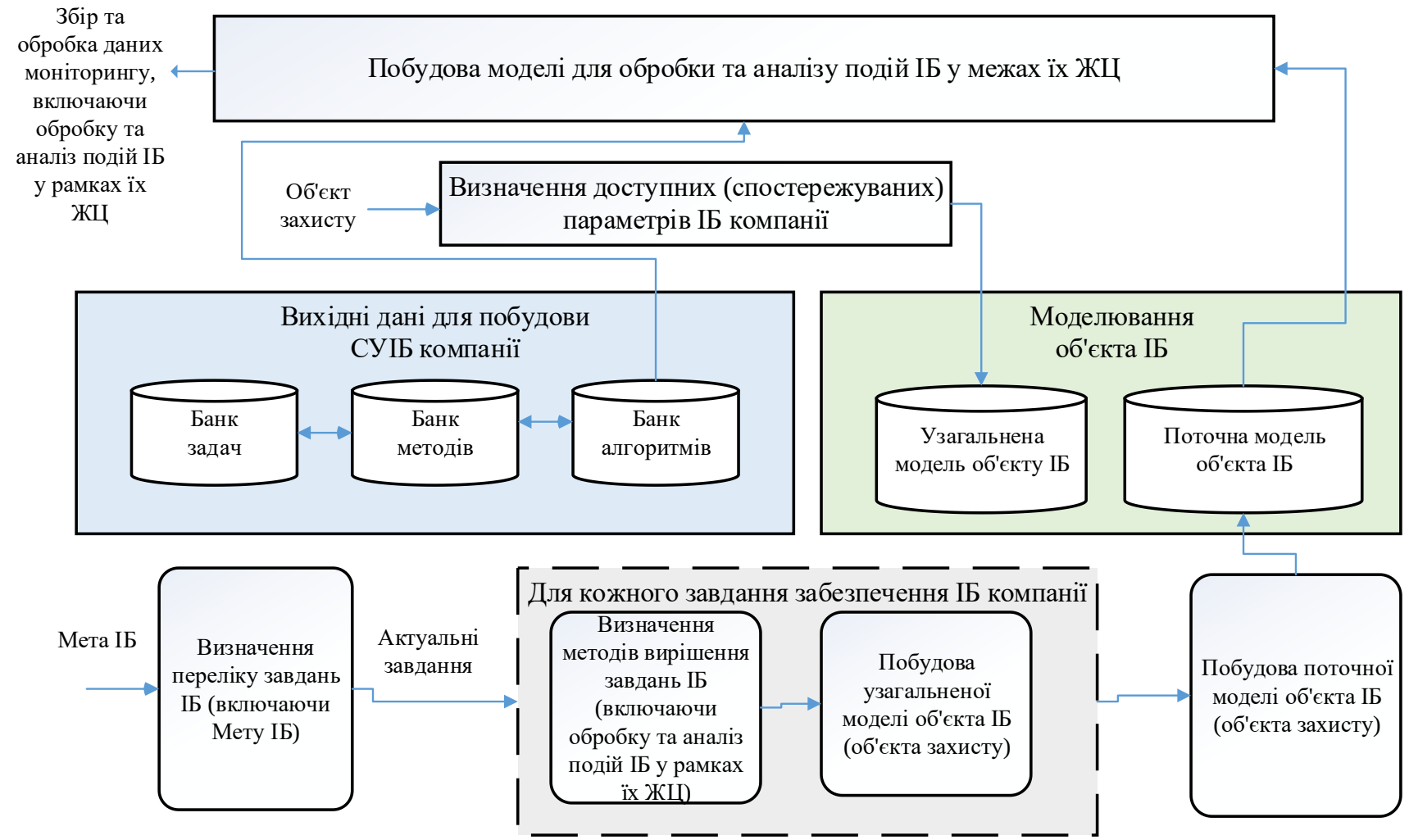
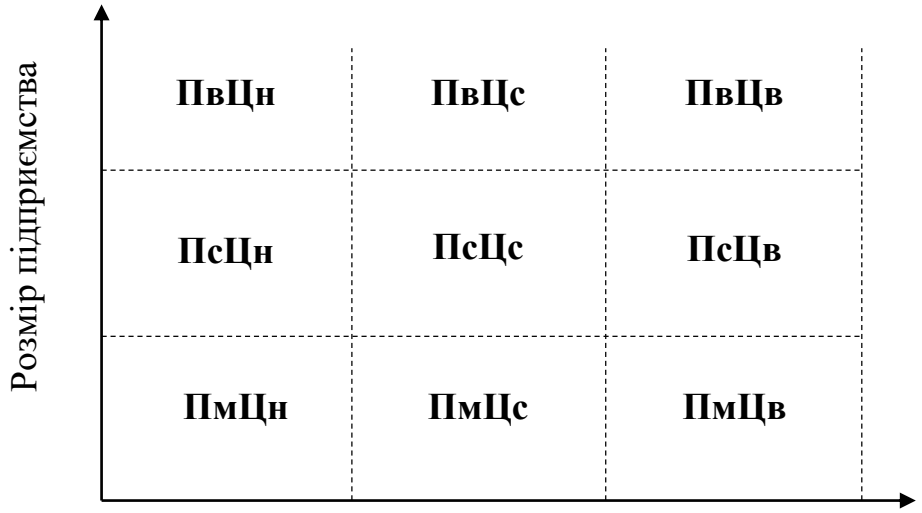


Рис. 5. Розширена схема адаптивного моніторингу інформаційної безпеки

Джерело: складено автором



П (м, с, в) – підприємство (мале, середнє, велике);

Ц (н, с, в) – рівень цифровізації процесів (низький, середній, високий)

Рис. 6. Типологія підприємств, що визначає вибір організаційно-економічних заходів захисту корпоративної інформації

Джерело: складено автором

Проведено імітаційне моделювання для конкретного прикладу розрахунку ефективності інвестування ІБ ОБІ. Це дозволило врахувати відносну невизначеність реальної ситуації з ІБ ОБІ. Показано, що проведені дослідження допоможуть практикам у сфері ІБ отримувати з допомогою викладеного в роботі підходу обґрунтовані рішення підвищення ефективності інвестиційних проектів у сфері ІБ для ОБІ. На відміну від існуючих, у запропонованій методиці враховані як прямі, так і непрямі чинники інвестиційних проектів у сфері ІБ ОБІ.

Уперше запропоновано модифікований метод аналізу ієрархій (МАІ), який відрізняється від стандартного, застосуванням апарату теорії нечітких множин та нейронних мереж (рис. 7), що дає можливість менеджменту приймати обґрунтовані управлінські рішення у сфері ІБ ОБІ.

Продемонстровано, що оцінку рівня ІБ для ОБІ доцільно проводити на основі оцінювання результативності безлічі критеріїв МАІ з використанням як метрик оцінювання, як стандартних чисельних метрик ІБ, так і метрик, запропонованих експертами з ІБ і погоджених з менеджментом ОБІ (табл. 2).

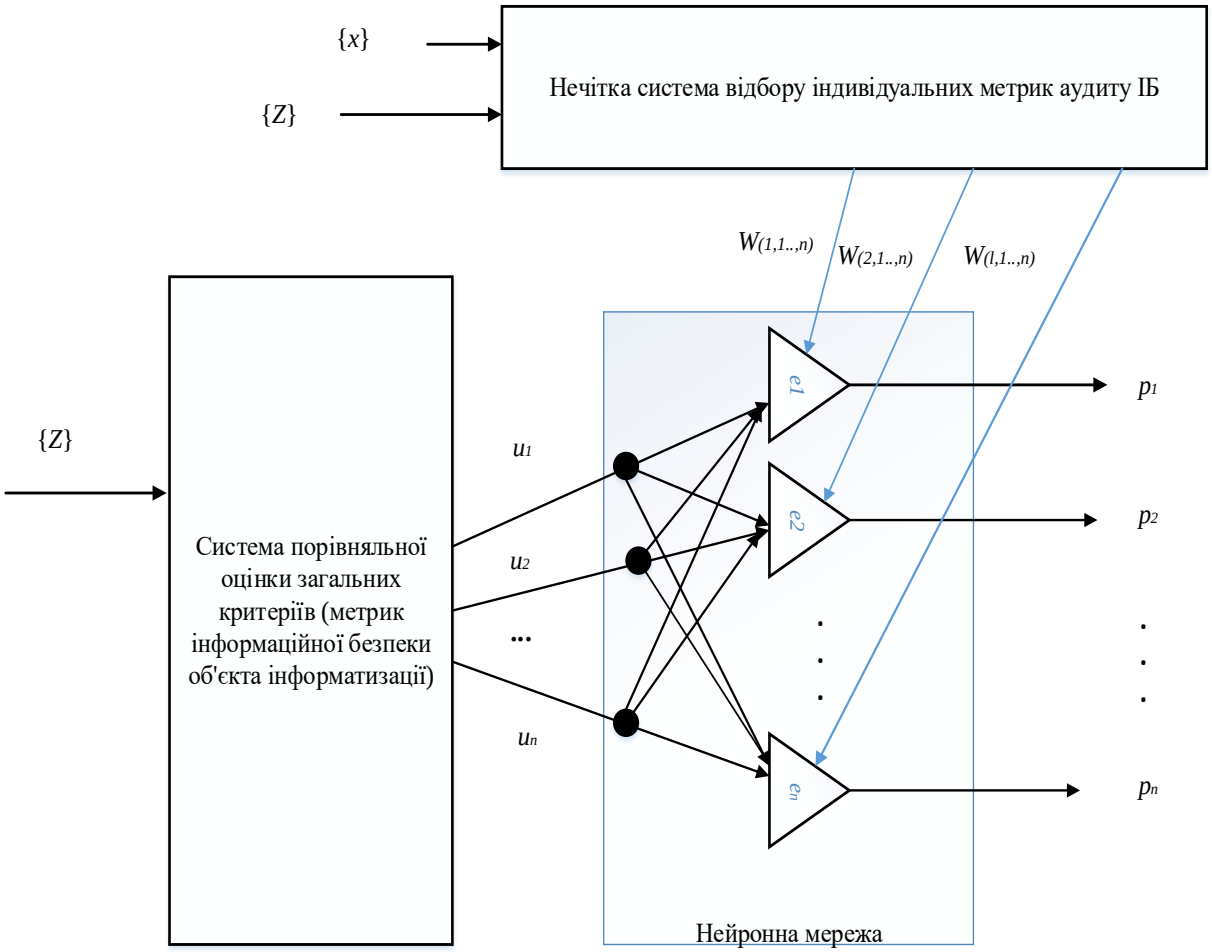


Рис. 7. Концептуальна структура нейро-нечіткої системи для модифікованого методу аналізу ієрархій

Джерело: складено автором

Таблиця 2

Загальні та індивідуальні метрики під час проведення аудиту ІБ

Загальні метрики ІБ	
1	Метрики, що характеризують хости та їх зв’язність
2	Відсоток критичних додатків
3	Середній час на усунення вразливості
…	….
N	Загальний виграш та очікувані річні втрати
Індивідуальні метрики ІБ (відібрано для аудиту ІБ для конкретного ОБІ)	
1	Імовірнісні заходи вразливості, що показують наскільки ймовірне виникнення вразливості нульового дня за певний період часу
2	Забезпечення максимальної повноти переліку інформаційних активів у аспекті додаткової інформації про загрози ІБ
3	Визначення ступеня реалізації міри (засобу) забезпечення ІБ
…	….
M	Установлений бізнес-ризик

Джерело: складено автором

Отримані рішення спрямовані на підвищення не лише власне ІБ ОБІ, а й у кінцевому підсумку оптимізують систему управління ОБІ, скорочують витрати й підвищують ефективність бізнес-процесів загалом. Продемонстровано, що застосування математичного апарату МАІ та відповідного програмного забезпечення, зокрема розробленої інтелектуальної системи, дозволяє підвищити ступінь достовірності результатів проведення комплексного аудиту ІБ ОБІ. Причому дане твердження справедливе як для процедур внутрішнього аудиту ІБ ОБІ, так і для зовнішнього аудиту.

Доповнено метод аудиту ІБ, заснований на автоматизації процедур аудиту шляхом залучення для оцінки ризиків ІБ апарату байєсовських мереж та штучних нейронних мереж. Показано, що така комбінація дозволяє оперативно в ході АІБ визначати актуальні ризики ІБ ОБІ. При цьому як вихідна інформація використовуються дані з датчиків/сенсорів різних апаратно-програмних засобів захисту інформації в сегментах розподілених обчислювальних мереж ОБІ. Показано, що автоматизація процедур аудиту ІБ на основі застосування байєсовських мереж та штучних нейронних мереж дозволяє адміністратору ІБ розподілених обчислювальних мереж своєчасно динамічно реагувати на загрози.

ВИСНОВКИ

У дисертаційній роботі здійснено теоретичне узагальнення та запропоновано нове розв’язання важливої наукової проблеми забезпечення ефективного захисту корпоративної інформації в умовах бурхливого розвитку інформаційних технологій. Результати досліджень дали змогу сформулювати концептуальні, теоретико-методологічні та науково-практичні висновки, спрямовані на вирішення завдань дисертації відповідно до визначеної мети.

1. Ураховуючи посилення ролі інформації у функціонуванні суспільства та економічних системах різного рівня, ускладнення структури та обсягу інформаційних потоків у системі прийняття управлінських рішень, інформаційні потоки та інформаційні процеси мають єдину природу, формуючи корпоративний інформаційний простір, що є цілісним системним утворенням. На основі аналізу, синтезу та розвитку наявних підходів уточнено зміст поняття корпоративного інформаційного простору як організованої системи інформації та інформаційних процесів корпорації, яка є станом та результатом її функціонування, способом її розвитку та представлення. Результати дослідження і використання системного підходу дозволили виокремити сутнісну ознаку корпоративного інформаційного простору «спосіб розвитку суб’єкта» та дали змогу побудувати його структуру, що включає: суб’єктів, семантичну складову, інформаційну інфраструктуру, регламенти та норми. Уточнення і доповнення категорій, що утворюють сутнісні ознаки та систему елементів корпоративного інформаційного простору, сприяло розвитку теоретико-методологічних положень та формуванню практичного інструментарію його захисту.

2. Розвиток корпоративного інформаційного простору впливає на трансформацію структури самої корпорації: її межі розмиваються, формуються

сучасні мережеві організаційні структури, що мають більш демократичний, гнучкий та адаптивний характер. Ідентифіковано основні етапи еволюції корпоративного інформаційного простору, зокрема: «паперовий», «автоматизований» і «мережевий». Доведено, що мережевість та розмитість меж корпоративного інформаційного простору розширює уявлення про його функціонування та зумовлює трансформацію самих корпорацій, що розширює уявлення про його функціонування та стає теоретичним підґрунтям для розроблення концепції формування корпоративної інформаційної безпеки, вироблення практичних рекомендацій щодо її формування на корпоративному рівні.

3. Ефективний розвиток підприємства значною мірою потребує врахування всіх компонентів корпоративного інформаційного простору і організації ефективної діяльності із забезпечення інформаційної безпеки. Визначення та синтез параметрів корпоративного інформаційного простору, зокрема: інтенсивності інформаційного обміну, насиченості інформаційних полів, рівня цифровізації, цифрової компетентності персоналу, рівня корпоративної інформаційної культури та доведення взаємообумовлюючої залежності між ними та функціями корпоративного інформаційного простору (інтегруючої, комунікативної, актуалізуючої, соціальної, навчальної, інноваційної, акселеруючої), дозволяють у цілому підвищувати результати діяльності за рахунок більш ефективного використання всього пулу ресурсів, а також здійснювати перманенте вдосконалення параметрів корпоративного інформаційного простору. Захист корпоративної інформації пов’язаний із захистом корпоративного інформаційного простору від різноманітних загроз з метою збереження високої якості його параметрів та забезпечення можливості ефективно виконувати ним свої функції, дозволили узагальнити та систематизувати класифікації загроз інформаційній безпеці підприємства та визначення змісту поняття «захист корпоративної інформації» як системи принципів, методів та процесів протидії загрозам інформаційній безпеці підприємства, які спрямовуються на порушення функціонування корпоративного інформаційного поля і передбачає їх ідентифікацію, аналіз, попередження та нейтралізацію.

4. Досягнення цільових параметрів системи захисту корпоративної інформації потребує розробки та впровадження в діяльність корпорацій дієвих механізмів протидії загрозам інформаційній безпеці підприємства, які узгоджуватимуться із сучасними концептуальними положеннями ефективності функціонування економічних систем. Постійне нарощення загроз інтересам підприємства, високий рівень флуктуацій зовнішнього середовища, необхідність постійної ідентифікації достатності зусиль в удосконаленні системи управління та здійснення їх порівняльної оцінки обумовили систематизацію видової трансформації економічної ефективності управління підприємством ефективності управління підприємством за елементами його управління: ефективність структурних підрозділів управління; ефективність процесів управління; ефективність центрів відповідальності; ефективність управлінського персоналу; ефективність управлінських рішень, яка суттєво детермінує ефективність функціонування підприємства та дозволяє сформулювати нову парадигму

«економічної ефективності захисту корпоративної інформації», як міри економічного ефекту витрачених ресурсів на реалізацію системи заходів з ідентифікації, аналізу, попередження та нейтралізації загроз порушення функціонування корпоративного інформаційного поля.

5. Ризикозахищеність системи інформаційної безпеки корпорацій характеризується відсутністю комплексного підходу до модернізаційних заходів, які мають охоплювати основні напрями їх функціонування з метою урахування релевантності точок контролю функцій системи управління інформаційною безпекою корпорацій. Базис концепції формування корпоративної інформаційної безпеки становить конвергенція позитивістської та нормативної економічних теорій, системного, процесного, проєктного підходів в управлінні та концепції динамічних компетентностей, що обґрунтовує методологію формування інформаційної безпеки: принципи та основні елементи механізму забезпечення інформаційної безпеки корпорацій. Структурні компоненти концепції формування інформаційної безпеки корпорацій ґрунтуються на синергетичному підході щодо індивідуалізації цілевизначення корпоративної інформаційної безпеки на різних підприємствах і окреслення підходів до управління нею, вибору методів управління інформаційною безпекою залежно від особливостей внутрішнього і зовнішнього середовища, узгодженості дій внутрішніх суб'єктів та посиленню взаємодії із зовнішніми суб'єктами інформаційної безпеки, ефективнішому використанню наявного ресурсного забезпечення та пошуку нових невикористаних раніше резервів для виконання поставлених завдань.

6. Основними домінантними чинниками формування базису корпоративної політики інформаційної безпеки в глобальному бізнес-середовищі слід вважати: створення єдиного цифрового корпоративного бізнес-простору, зростання швидкості впровадження цифрових бізнес-стратегії з високим рівнем технологічного розгортання та інтенсивності порушень стійкості системи захисту корпоративної інформації. Врахування цих чинників сприяє ефективному протіканню забезпечуюючих процесів корпоративної політики інформаційної безпеки, систематизації її видів шляхом визначення стратегічної і тактичної її складової, фокусування уваги на підвищення економічної ефективності корпоративної політики інформаційної безпеки за рахунок її гнучкого реагування на зміну стратегічних цілей, попередження та ліквідації наслідків впливу дестабілізуючих чинників на діяльність корпоративних структур.

7. Важливою складовою системи управління інформаційною безпекою корпорацій є забезпечення економічної ефективності корпоративної інформаційної безпеки. Складність застосування єдиної методики для формування вичерпного висновку щодо ефективності корпоративної інформаційної безпеки обумовлюється необхідністю виявлення та розв'язання ряду проблем, зокрема: необхідності обґрунтування принципів оцінювання та систематизації показників економічної ефективності; визначення чітких критеріїв оцінювання окремих показників; обґрунтування рекомендацій щодо логічної послідовності аналізу окремих показників; необхідності формування інтегрального або узагальнюючого показника ефективності корпоративної інформаційної безпеки. Методологічний підхід до оцінювання економічної ефективності захисту корпоративної інформації

включає: принципи оцінювання та систематизації показників; систему часткових показників економічної ефективності та критеріальну шкалу їх інтерпретації; узагальнюючу оцінку економічної ефективності захисту корпоративної інформації на основі поєднання інтегрального показника та показника прогресивності розвитку системи захисту КІ, структурно-логічну послідовність етапів оцінювання, дозволяє структурувати процес оцінки та запровадити дієві системи оцінювання економічної ефективності захисту корпоративної інформації ефективності захисту корпоративної інформації.

8. У міру зростання кількості злочинів у сфері незаконного (неправомірного) втручання в роботу інформаційних систем виявлення та боротьба з несанкціонованим доступом до інформаційних ресурсів стала однією з основних проблем для багатьох підприємств. Підхід до процедури визначення ознакового функціонального подання неправомірних дій комп'ютерного зловмисника шляхом формалізації ієрархічної схеми формування простору ознак несанкціонованого доступу до ресурсів ІС підприємства створює базис для подальшого синтезу інтелектуальної системи виявлення спроб НСД в умовах важкозрозумілих ознак або їх невеликого числа. Це дозволяє ефективно реалізувати первинну формалізацію неправомірних дій комп'ютерних зловмисників для подальшого математичного опису параметра ймовірності НСД .

9. Захист інформаційного простору підприємств від несанкціонованого доступу за допомогою ТЗР або від деструктивних впливів на інформаційні ресурси, передбачає застосування системи постійного збору, обробки, аналізу відповідних даних, що стосуються оцінки актуальності загроз витоку інформації з ТКПІ в умовах динамічного вдосконалення ТЗР. Автоматизація та систематизація комплексної оцінки ефекту захищеності інформації від витоків технічними каналами включає ПЗ, яке призначене для виміру ризиків втрати інформації, дозволяє ідентифікувати рівень захищеності ТКПІ підприємства та сприяє зниженню витрат на проведення вузькоспеціальних досліджень у питаннях щодо оцінки актуальності загроз витоку інформації з ТКПІ. Це вдосконалює процес оцінювання захищеності підприємств шляхом використання релевантних оцінок експертів.

10. Оцінка реального ефекту від інвестування в ІБ ОБІ є складним процесом, в зв'язку з тим, що існує великий перелік факторів для сегменту захисту інформації (ЗІ) та кібернетичної безпеки (КБ), зокрема: ландшафт кіберзагроз, що постійно змінюється; різноваріантні стратегії та тактики атакуючої сторони (комп'ютерних зловмисників); швидкий розвиток технічних засобів захисту інформації (ЗІ) та кібербезпеки (КБ) тощо. Ефективність заходів, спрямованих на підвищення ступеня захищеності та ІБ ОБІ не може бути дано лише на основі детермінованих оцінок та вимагає залучення ймовірнісних характеристик. Модель оцінювання економічної ефективності інвестицій на формування системи захисту корпоративної інформації, яка базується на оцінки попереджених збитків від кібератак на основі базисного показника розрахунку економічного ефекту від інвестування у ЗЗІ дозволить усунути суперечливість у питанні оцінювання ефективності заходів, спрямованих на забезпечення ІБ ОБІ.

11. Моніторинг ландшафту кібернетичних загроз продемонстрував інтенсивність мінливості та уразливості функціонування бізнесу. Деструктивний вплив інформаційних втрат супроводжуються зростаючою вартістю фінансових втрат. Аналіз статистичних даних показав, що результатом кібератак на приватних і юридичних осіб є витік облікових даних, даних платіжних карток, персональних даних. комерційної таємниці та медичної інформації, за секторальним розподілом атак превалюють державні установи, потім промислові та медичні підприємства. Зростання питомої ваги цифрової інформації обумовлюють практичну потребу в організаційній та технологічній модернізації систем захисту інформації, що передбачає математично-алгоритмічну та комп'ютерну підтримку процедури прийняття рішень у питаннях організаційно-економічного забезпечення ефективного захисту корпоративної інформації в контексті завдань менеджменту інформаційної безпеки (ІБ) підприємств.

12. Система управління інформаційною безпекою інтегрує окремі, часто розрізнені заходи, спрямовані на забезпечення захисту інформації та інформаційної безпеки підприємства. Ключовим процесом системи управління інформаційною безпекою підприємства є процес «Управління подіями». Діюча практика управління корпоративною інформаційною безпекою доповнена підпроцесом «Обробка подій», який удосконалює підхід до організації процесу управління подіями інформаційної безпеки корпорацій та дозволяє здійснювати комплексну деталізацію процесу управління подіями інформаційної безпеки корпорацій, врахувати їх життєвий цикл, заповнити потенційні прогалини інформації та спростити процедуру управління інформаційною безпекою корпорації в цілому.

13. Різноманіття завдань інформаційної безпеки корпорацій та динамічні особливості об'єктів захисту обумовили необхідність імплементації методології теорії систем та впровадження в діючу практику управління інформаційною безпекою корпорацій адаптивного моніторингу інформаційної безпеки, який базується на принципах: ієрархічної пов'язаності подій; цілісності та подібності подій інформаційної безпеки, включає процедури оброблення та аналізу подій інформаційної безпеки в межах їх життєвого циклу та дозволяє, не змінюючи методичний інструментарій, масштабувати даний підхід і адаптувати його до системи управління інформаційної безпеки різних підприємств.

14. Оцінка ефективності та результативності системи захисту корпоративної інформації включає порівняння рівня продуктивності з рівнем виконання бюджету щодо створення такої системи та здійснюється керівництвом підприємства з метою контролю за досягненням цілей та завдань функціонування інформаційної безпеки та визначення напрямів необхідних змін. Оцінка економічної ефективності системи захисту корпоративної інформації, яка побудована на принципах комплексності, урахуванні стадії розвитку корпоративних систем та життєвого циклу корпоративної інформації; об'єктивності; рентабельності та цифровізації, включає визначення ступеня досягнення максимально можливого прибутку корпоративними структурами та рейтингову шкалу оцінки ефективності системи захисту корпоративної інформації, дозволила посилити управлінські заходи у процесі формування стратегії та механізмів забезпечення комплексної системи корпоративної інформаційної безпеки при формування адекватних заходів,

спрямованих на виявлення та усунення проблем функціонування системи захисту корпоративної інформації, зменшення негативного впливу викликів і загроз інформаційної безпеці, попередження або мінімізацію можливих збитків.

15. Організаційно-економічне забезпечення захисту корпоративної інформації є комплексом взаємоузгоджених елементів (заходів) різної спрямованості та частоти застосування, які перебувають у постійній взаємодії, виступають частиною економічного механізму інформаційної безпеки, реалізуються на різних контурах управління (стратегічному, тактичному, оперативному рівнях) та інтегровані в систему загальнокорпоративного управління з метою досягнення визначених цілей. Класифікація елементів за функціональним напрямом (нормативно-правові, організаційні, соціально-економічні, програмно-апаратні) дозволяє диференційовано реалізовувати їх залежно від потреби спрямованості впливу на формування (зовнішнього середовища, внутрішньокорпоративні) та частоти застосування (перманентні, ситуативні). З метою здійснення вибору альтернатив організаційно-економічних заходів захисту корпоративної інформації запропоновано використовувати розроблену шкалу, яка базується на комбінації двох принципово важливих змінних «розмір підприємства підприємство (мале, середнє, велике) – рівень його цифровізації (низький, середній, високий)». Це дозволить підвищити ефективність організаційно-економічного забезпечення захисту корпоративної інформації на основі алгоритмізації управлінських дій з урахуванням релевантних факторів впливу.

16. Інтенсифікація змін ландшафту кіберзагроз пріоритетно обумовила трансформаційні зміни процедури проведення аудитів ІБ ОБІ та оперативного реагування на виявлені загрози в інформаційних системах, що можливо забезпечити на основі впровадження інтелектуальних систем підтримки прийняття рішень (ІСППР). Представлений алгоритм проведення аудиту ІБ включає вимоги щодо використання відібраних аудиторами пріоритетних метрик ІБ, контролю виявлених відхилень в якісних характеристиках відібраної метрики ІБ, формування правил відбору та постійного моніторингу об’єктивних причин заміни раніше відібраних метрик ІБ. Методичний підхід до моделювання системи оцінювання рівня інформаційної безпеки для об’єктів інформатизації ґрунтується на методі аналізу ієрархій (МАІ), що, у свою чергу, дозволяє враховувати загальні та індивідуальні критерії оцінки (метрики ІБ) ступеня кібербезпеки ОБІ. Модифікований метод аналізу ієрархій, який базується на застосуванні апарату теорії нечітких множин та нейронних мереж, дозволяє підвищити обґрунтованість прийняття управлінських рішень у сфері ІБ щодо оптимізації системи управління ОБІ, скорочення витрат та підвищення адаптивності реалізації бізнес-процесів ОБІ.

17. Оцінка ризиків ІБ починається на стадії проєктування ІС для ОБІ з використанням апарату нечіткої логіки (НЛ) та ШНМ у процедурі аудиту ІБ. Методичний підхід оцінки ризиків інформаційної безпеки підприємства в автоматизованих системах захисту корпоративної інформації базується на поєднанні стандартних чисельних та експертних метрик оцінювання ІБ, який дозволяє застосувати контрзаходи захисту ІБ ОБІ та побудувати ефективну СУІБ, що превентивно адаптується до нових загроз. Комбіноване використання апарату

Байєсовських мереж та штучної нейронної мережі дозволяє автоматизувати процедури аудиту ІБ. Результатом автоматизації є підтримка варіантів технічних рішень, які забезпечують можливість адміністратору ІБ РОМ діяти на випередження.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Монографії:

1. Чубаєвський В. І. Корпоративна інформаційна безпека : монографія / В.І. Чубаєвський. Київ : Держ. торг.-екон. ун-т, 2022. 272 с. (14 друк. арк.).

Статті у наукових фахових виданнях України, у виданнях України, які включено до міжнародних наукометричних баз:

2. Чубаєвський В. Світова практика управління подіями інформаційної безпеки корпорацій. *Зовнішня торгівля: економіка, фінанси, право*. 2022. № 6. С. 73–82. (0,9 друк. арк.; *наукове фахове видання України, категорія «Б»*).

3. Чубаєвський В. І. Методичний підхід до оцінки економічної ефективності системи захисту корпоративної інформації. *Електронний журнал «Ефективна економіка»*. 2022. № 11. URL: https://nayka.com.ua/index.php/ee/article/view/730/738 (дата звернення: 21.11.2022). (0,6 друк. арк.; *наукове фахове видання України, категорія «Б»*).

4. Чубаєвський В. І. Прогресивність розвитку системи захисту корпоративної інформації. *Економіка та суспільство*. 2022. № 44. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1793 (дата звернення: 01.11.2022). (0,6 друк. арк.; *наукове фахове видання України, категорія «Б»*).

5. Чубаєвський В. Корпоративний інформаційний простір: сутність та еволюція. *Scientia Fructuosa (Вісник Київського національного торговельно-економічного університету)*. 2022. № 4. С. 84–97. (1,1 друк. арк.; *наукове фахове видання України, категорія «Б»*).

6. Чубаєвський В. І. Особливості формування системи захисту інформаційних ресурсів корпоративних структур. *Фаховий електронний науково-практичний журнал «Проблеми сучасних трансформацій. Серія: економіка та управління»*. 2022. № 5. URL: https://reicst.com.ua/pmt/article/view/2022-5-04-10/2022-5-04-10 (дата звернення: 01.11.2022). (0,5 друк. арк.; *наукове фахове видання України, категорія «Б»*).

7. Чубаєвський В. І. Методи управління корпоративною інформаційною безпекою. *Економіка та суспільство*. 2022. № 43. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1732 (дата звернення: 01.11.2022). (0,7 друк. арк.; *наукове фахове видання України, категорія «Б»*).

8. Chubaievskyi V., Blakyta H., Matusova O., Adamenko V., Hamula I. Assessing the state of the corporate information area in Ukraine. *Міждисциплінарні дослідження складних систем = Interdisciplinary Studies of Complex Systems* : Збірник наукових праць. Київ : Вид-во НПУ імені М. П. Драгоманова, 2022. № 20. С. 35–45. (1,0 друк. арк.; *особистий внесок: запропоновано методичний інструментарій оцінки стану корпоративної інформаційної сфери країни* – 0,2 друк. арк.; *Web of Science*).

9. Chubaievskyi V., Tereshchenko E., Andryeyeva V., Stoianenko I. Model for assessing technological resources in the economic security of business in the process of European integration. *Information-analytical journal «Economics. Finances. Law»*. 2022. № 8. P. 13–16. (0,4 друк. арк.; *особистий внесок: запропонована модель оцінки технологічних ресурсів економічної безпеки бізнесу* – 0,1 друк. арк.; *наукове фахове видання України, категорія «Б», Index Copernicus*).

10.Chubaievskyi V., Blakyta H., Bogma O., Shtuler I., Batrakova T. Protection of information resources as an integral part of economic security of the enterprise. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetuthis*. 2022. № 4. P. 117–122. (0,5 друк. арк.; *особистий внесок: обґрунтовано модель побудови системи захисту інформації підприємств* – 0,1 друк. арк.; *наукове фахове видання України, категорія «А», Scopus, Index Copernicus*).

11.Чубаєвський В., Десятко А., Криворучко О., Лахно В., Блозва А., Місюра М. Застосування СППР у завданнях організаційно-економічного забезпечення захисту інформації. *Інформаційні технології та суспільство*. 2022. № 2(4). С. 107–116. (0,6 друк. арк.; *особистий внесок: описано процедури формалізації завдання оптимізації системи захисту інформації* – 0,1 друк. арк.; *наукове фахове видання України, категорія «Б»*).

12.Чубаєвський В. І., Жук Т. В. Економічна ефективність інформаційної безпеки підприємств торгівлі. *Scientia Fructuosa (Вісник Київського національного торговельно-економічного університету)*. 2022. № 1. С. 106–117. (1,0 друк. арк.; *особистий внесок: обґрунтовано вибір методів оцінки економічної ефективності інформаційної безпеки для підприємств торгівлі* – 0,5 друк. арк.; *наукове фахове видання України, категорія «Б»*).

13.Чубаєвський В. І., Богма О. С., Сілакова Г. В. Методика оцінки ефективності систем захисту корпоративної інформації вітчизняних підприємств. *Економічний простір*. 2022. № 177. С. 56–61. (0,6 друк. арк.; *особистий внесок: запропоновано інтегральну методику оцінювання рівня ефективності системи захисту корпоративної інформації підприємства, яка передбачає розрахунок інтегральних показників за кожною виділеною складовою системи захисту корпоративної інформації підприємства й загального інтегрального показника* – 0,2 друк. арк.; *наукове фахове видання України, категорія «Б»*).

14.Чубаєвський В. Стратегічні орієнтири формування корпоративної політики інформаційної безпеки. *Причорноморські економічні студії*. 2021. Вип. 72. (Ч. 2). С. 24–30. (0,4 друк. арк.; *наукове фахове видання України, категорія «Б»*).

15.Чубаєвський В., Лахно В., Ахметов Б., Криворучко О., Касаткін Д., Десятко А., Литовченко Т. Оптимізації резерву обладнання для інтелектуальних автоматизованих систем. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2021. Т. 2. № 14. С. 87–99. (0,7 друк. арк.; *особистий внесок: запропоновано алгоритми для нейромережевого аналізатора кібербезпеки* – 0,1 друк. арк.; *наукове фахове видання України, категорія «Б»*).

16.Чубаєвський В., Лахно В., Криворучко О., Касаткін Д., Десятко А., Блозва А., Гусєв Б. Методика мінімізації витрат на побудову багатоконтурної системи захисту на основі генетичного алгоритму. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2021. Т. 1. № 13. С. 16–28. (1,1 друк. арк.;

особистий внесок: обґрунтовано оптимальні параметри компонентів СЗІ з урахуванням обраних експертом пріоритетних метрик кібербезпеки ОБІ – 0,3 друк. арк.; *наукове фахове видання України, категорія «Б»*).

17.Чубаєвський В., Лахно В., Криворучко О., Касаткін Д., Десятко А., Блозва А. Ефективність методики розрахунку показників інвестицій в системи інформаційної безпеки об'єктів інформатизації. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2021. Т. 4. № 12. С. 96–107. (1,0 друк. арк.; *особистий внесок: обґрунтовано можливість і необхідність отримання необхідних даних, що сприяють достовірній оцінці ефективності заходів, спрямованих на підвищення інформаційної безпеки компанії* – 0,2 друк. арк.; *наукове фахове видання України, категорія «Б»*).

18.Чубаєвський В., Волосович С. Безпека корпоративної інформації в екосистемі FinTech. *Foreign trade: Economics, Finance, Law*. 2021. Т. 119. № 6. С. 98–108. (0,8 друк. арк.; *особистий внесок: проаналізовано подвійну природу кібербезпеки, що одночасно є складовою FinTech і забезпечує захист корпоративних інформаційних систем учасників екосистеми FinTech* – 0,4 друк. арк.; *наукове фахове видання України, категорія «Б»*).

Статті у закордонних виданнях:

19.Lakhno V., Akhmetov B., Mohylnyi H., Chubaievskyi V., Kryvoruchko O., Desiatko A. Multi-criterial optimization composition of cyber security circuits based on genetic algorithm. *Journal of Theoretical and Applied Information Technologythis*. 2022. Vol. 100. № 7. P. 1996–2006. (0,9 друк. арк.; *особистий внесок: запропонована методика багатокритеріальної оптимізації витрат на систему захисту інформації об'єкта інформатизації, яка полягає в застосуванні генетичного алгоритму VEGA (Vector Evaluated Genetic Algorithm)* – 0,1 друк. арк.; *Scopus*).

20.Lakhno V., Bereke M., Adilzhanova S., Chubaievskyi V., Desiatko A., Palaguta K. Genetic algorithm for solving the problem of scaling a cloud-oriented object of informatization. *Journal of Theoretical and Applied Information Technologythis link is disabled*. 2022. Vol. 100. № 6. P. 1693–1705. (1,2 друк. арк.; *особистий внесок: запропоновано генетичний алгоритм розв'язання задачі масштабування хмароорієнтованого об'єкта інформатизації* – 0,2 друк. арк.; *Scopus*).

21.Lakhno V., Blozva A., Kasatkin D., Chubaievskyi V., Tyshchenko D., Brzhanov R. Experimental studies of the features of using waf to protect internal services in the zero trust structure. *Journal of Theoretical and Applied Information Technologythis*. 2022. Vol. 100. № 3. P. 705–721. (1,8 друк. арк.; *особистий внесок: досліджено використання WAF у захисті внутрішніх сервісів у структурі Zero Trust* – 0,3 друк. арк.; *Scopus*).

22.Akhmetov B., Lakhno V., Chubaievskyi V., Kaminskyi S., Adilzhanova S., Ydyryshbayeva M. Automation of Information Security Risk Assessment. *International Journal of Electronics and Telecommunicationsthis*. 2022. Vol. 3. № 68. P. 549–555. (0,6 друк. арк.; *особистий внесок: розроблено метод аудиту інформаційної безпеки для розподільної числової мережі об'єкта інформатизації* – 0,1 друк. арк.; *Scopus*).

23.Lakhno V., Akhmetov B., Mazaraki A., Chubaievskyi V., Desiatko A. Methodology for assessing the effectiveness of measures aimed at ensuring information

security of the object of informatization. *Journal of Theoretical and Applied Information Technologythis*. 2021. Vol. 14. № 99. P. 3417–3427. (1,0 друк. арк.; *особистий внесок: запропонована методика розрахунку показників від інвестиційних заходів у рамках підвищення метрик ІБ ОБІ* – 0,2 друк. арк.; *Scopus*).

24.Sahun A., Khaidurov V., Lakhno V., Opirskyy I., Chubaievskyi V., Kryvoruchko O., Desiatko A. Devising a Method for improving crypto resistance of the symmetric block cryptosystem Rc5 using nonlinear shift functions. *Eastern-European Journal of Enterprise Technologies*. 2021. Vol. 5. № 9. P. 17–29. (1,2 друк. арк.; *особистий внесок: розроблено алгоритм, що може бути застосований в комп'ютерних системах з низькою обчислювальною продуктивністю* – 0,2 друк. арк.; *Scopus*).

Опубліковані праці апробаційного характеру:

25.Lakhno V., Kasatkin D., Desiatko A., Chubaievskyi V., Tsuitsuira S., Tsuitsuira M. Indicators Systematization of Unauthorized Access to Corporate Information / Rajakumar G., Du K. L., Vuppalapati C., Beligiannis G. N. (eds) *Intelligent Communication Technologies and Virtual Mobile Networks* : Lecture Notes on Data Engineering and Communications Technologies. Singapore : Springer, 2023. Vol. 131. P. 569–580. (0,8 друк. арк.; *особистий внесок: запропоновано підхід до процедури формалізації ознакового функціонального подання неправомірних дій комп'ютерного зловмисника під час реалізації функцій несанкціонованого доступу до ресурсів інформаційних систем компаній та підприємств* – 0,1 друк. арк.; *Scopus*).

26.Чубаєвський В. І. Особливості оцінки економічної ефективності інвестування в об'єкти інформаційної безпеки корпорацій. *Сучасні проблеми економіки та бізнесу* : матеріали XII Міжнародної науково-практичної конференції (Київ, 10–11 листопада 2022 р.). Київ : НАУ, 2022. С. 220–222. (0,1 друк. арк.).

27.Чубаєвський В. І. Реалізація методичного підходу до оцінки економічної ефективності системи захисту корпоративної інформації. *Сучасні тренди соціально-економічних перетворень та інтелектуалізації суспільства в умовах сталого розвитку* : тези доповідей Міжнародної науково-практичної конференції (10 листопада, м. Запоріжжя). Запоріжжя : НУ «Запорізька політехніка», 2022. С. 372–374 (0,1 друк. арк).

28.Lakhno V., Mazaraki A., Kasatkin D., Kryvoruchko O., Khorolska K., Chubaievskyi V. Models and Algorithms for Optimization of the Backup Equipment for the Intelligent Automated Control System Smart City. *Inventive Communication and Computational Technologies*. *Lecture Notes in Networks and Systems* : Proceedings of ICICCT 2022 / Editors: G. Ranganathan, Xavier Fernando, Álvaro Rocha. Singapore : Springer, 2022. Vol. 383. P. 749–762. (1,0 друк. арк.; *особистий внесок: запропоновано моделі та алгоритми оптимізації кібербезпеки інтелектуальної автоматизованої системи управління Smart City* – 0,1 друк. арк.; *Scopus*).

29.Chubaievskyi V. Directions of assessment of technological resources of economic security of business in the process of European Integration. *Стратегічні орієнтири розвитку економіки, фінансів, обліку і права* : збірник тез доповідей міжнародної науково-практичної конференції (Полтава, 30 липня 2022 р.). Полтава : ЦФЕНД, 2022. С. 17–19. (0,2 друк. арк.).

30.Lakhno V., Kozlovskyi V., Klobukov V., Chubaievskyi V., Tyshchenko D. Software Package for Information Leakage Threats Relevance Assessment. *Lecture Notes in Networks and Systemsthis* : Computer Science On-line Conference / Conference Paper. 2022. Vol. 503. P. 290–301. (1,0 друк. арк.; *особистий внесок: запропоновано методологічний підхід, який дозволяє автоматизувати та систематизувати прояви ефекту захищеності інформації від витоків по технічних каналах передачі* – 0,2 друк. арк.; *Scopus*).

31.Lakhno V., Malyukov V., Kryvoruchko O., Chubaievskyi V., Misiura M., Pashorin V. Methodology for placing components of a video surveillance system for smart city based on a composite cost optimization model. *Lecture Notes in Networks and Systemsthis* : Computer Science On-line Conference / Conference Paper. Springer, Cham, 2022. Vol. 501. P. 13–23. (0,8 друк. арк.; *особистий внесок: розроблено новий клас білінійних диференціальних ігор в нечіткій постановці, що можуть бути застосовані до фізичних систем захисту в корпоративному середовищі* – 0,1 друк. арк.; *Scopus*).

32.Lakhno V., Akhmetov B., Chubaievskyi V., Desiatko A., Palaguta K., Blozva A., Chasnovskyi Y. Information security audit method based on the use of a neuro-fuzzy system. *Proceedings of the 5th Computational Methods in Systems and Software 2021*. Springer, Cham, 2021. P. 171–184. (1,4 друк. арк.; *особистий внесок: запропоновано модифікований метод аналізу ієрархій, на основі застосування апарату теорії нечітких множин та нейронних мереж* – 0,2 друк. арк.; *Scopus*).

33.Чубаєвський В. І., Франчук Т. М. Проблеми захисту персональних даних в електронно-інформаційному середовищі. *Кібергігієна. Кібербезпека. Безпека держави* : матеріали наукових семінарів (м. Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. Київ : Київ. нац. торг.-екон. ун-т, 2020. С. 34–36. (*особистий внесок: запропоновано методи діагностування загроз несанкціонованого доступу до персональних даних* – 0,1 друк. арк.).

34.Чубаєвський В. І., Терешенко Е. Ю. Особливості моніторингу оцінки інформаційної безпеки України. *Інформаційно-аналітичне забезпечення управління фінансово-економічною безпекою держави, регіону, суб'єктів господарювання в умовах COVID-19* : матеріали X Міжнар. наук.-практ. конф., Харків, 18-19 листопада 2021 року / Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2021. С. 294–297. (*особистий внесок: визначено склад показників системи моніторингу оцінки інформаційної безпеки* – 0,1 друк. арк.).

35.Чубаєвський В., Криворучко О., Десятко А. Оцінка якості програмного забезпечення інформаційно-управляючих систем. *Глобалізаційні виклики розвитку національних економік* : тези доповідей II Міжнар. наук.-практ. конф. (Київ, 19 жовтня 2021 р.) / відп. ред. А. А. Мазаракі. Київ : Київ. нац. торг.-екон. ун-т, 2021. С. 278–281. (*особистий внесок: оцінка захищеності програмного забезпечення інформаційно-управляючих систем* – 0,1 друк. арк.).

36.Лахно В., Ахметов Б., Чубаєвський В., Криворучко О., Десятко А., Пашорін В. Оцінювання ефективності заходів щодо забезпечення інформаційної безпеки об'єкта інформатизації. *Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні 2021* : збірник матеріалів

IX Міжнар. наук.-практ. інтернет конф., м. Київ, 13–14 трав. 2021 р. Київ : НУБіП України, 2021. С. 45–48. (*особистий внесок: обґрунтування системи показників для оцінювання ефективності заходів щодо забезпечення інформаційної безпеки об'єкта інформатизації* – 0,1 друк. арк.).

37.Чубаєвський В., Макоєдова В. Застосування багаторівневого підходу як засіб протидії кіберзагрозам. *Проблеми кібербезпеки інформаційно-телекомунікаційних систем* : Збірник матеріалів доповідей та тез; м. Київ, 15-16 квітня 2021 року; Київський національний університет імені Тараса Шевченка / Редкол.: О.К. Закусило. (голова) та ін. Київ : ВПЦ «Київський університет», 2021. С. 18-19. (*особистий внесок: обґрунтування застосування багаторівневого підходу для протидії кіберзагрозам* – 0,1 друк. арк.).

АНОТАЦІЯ

Чубаєвський В.І. Економічна ефективність систем захисту корпоративної інформації. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора наук за спеціальністю 08.00.04 – економіка та управління підприємствами (за видами економічної діяльності) – Державний торговельно-економічний університет, Київ, 2023.

У дисертації досліджено теоретико-методологічні засади та методичні підходи до формування економічно-ефективної системи захисту корпоративної інформації. Визначено основні сутнісні характеристики та зміст корпоративного інформаційного простору; ідентифіковано етапи його еволюції та особливості розвитку на сучасному етапі. З'ясовано, що корпоративний інформаційний простір характеризується єдністю та взаємообумовленістю окремих елементів, сформульовано бачення структури корпоративного інформаційного простору, як єдності суб'єктів, семантичної складової, інформаційної інфраструктури, регламентів та норм. Визначено зміст корпоративної інформаційної безпеки, сформульовано концептуальне бачення місця захисту корпоративної інформації в забезпеченні ефективного економічного розвитку підприємства на основі доведеної взаємообумовлюючої залежності між параметрами та функціями корпоративного інформаційного простору (КІП); розширено перелік параметрів КІП, ідентифіковано систему функцій КІП та сформульоване авторське бачення сутності захисту корпоративної інформації.

Представлено теоретичний концепт сутності економічної ефективності управління підприємством на основі нової авторської трактовки змісту «управління підприємством», систематизовано основні методичні підходи до оцінювання економічної ефективності захисту корпоративної інформації; обґрунтовано авторську концепцію формування корпоративної інформаційної безпеки, систематизовано та узагальнено напрями корпоративної політики інформаційної безпеки через обґрунтування домінантних чинників формування її базису в глобальному бізнес-середовищі. Розроблено методологічний підхід до оцінювання економічної ефективності захисту корпоративної інформації, який включає: принципи оцінювання та систематизації показників; систему часткових

показників економічної ефективності та критеріальну шкалу їх інтерпретації; узагальнюючу оцінку економічної ефективності захисту корпоративної інформації на основі поєднання інтегрального показника та показника прогресивності розвитку системи захисту КІ (корпоративної інформації), структурно-логічну послідовність етапів оцінювання, що створює основу для запровадження дієвих систем оцінювання економічної ефективності захисту корпоративної інформації.

Розроблено методологічний підхід до процедури формалізації ознакового функціонального подання неправомірних дій комп'ютерного зловмисника в ході реалізації функцій НСД до ресурсів ІС підприємств; підхід до організації процесом управління подіями інформаційної безпеки (ІБ) для підприємства; підхід до адаптивного моніторингу інформаційної безпеки; методичні підходи до моделювання системи оцінювання рівня інформаційної безпеки (ІБ) для об'єктів інформатизації (ОБІ), наукові підходи до створення моделі, що описує процедуру формалізації завдання оптимізації системи захисту інформації (СЗІ) підприємства, розроблено та описано інтелектуальну систему оцінки загроз витоку інформації щодо технічних каналів передачі інформації, в основу якої покладено метод аудиту інформаційної безпеки.

Ключові слова: економічна ефективність, економічна безпека, корпоративна інформаційна безпека, захист корпоративної інформації, корпоративний інформаційний простір, політика захисту корпоративної інформації.

SUMMARY

Chubaevsky V.I. Economic efficiency of corporate information protection systems. – Qualifying scientific work on manuscript rights.

Dissertation for the degree of Doctor of Sciences in the specialty 08.00.04 – economics and management of enterprises (by types of economic activity) – State University of Trade and Economics, Kyiv, 2023.

The dissertation examines theoretical and methodological principles and methodological approaches to the formation of economically efficient system for corporate information protection. We determined the main essential characteristics and content of the corporate information space; identified the stages of its evolution and features of development at the present phase; formulated the vision of corporate information space structure. Based on the proven interdependence between the parameters and functions of the corporate information space, the corporate information security content is determined and a conceptual vision of the place of corporate information protection in ensuring effective economic enterprise development is formulated. We presented the theoretical concept of the essence of the economic efficiency in enterprise management; systematized the main methodical approaches to evaluating the economic efficiency of corporate information protection; substantiated the author's concept of corporate information security formation; systematized and summarized the directions of corporate information security policy; developed a methodological approach to evaluating the economic effectiveness of corporate information protection. We developed methodological approaches to the procedure of formalization for computer attacker illegal actions indicative functional presentation;

investigated the organization of managing information security events, adaptive monitoring, and level assessment.

Keywords: economic efficiency, economic security, corporate information security, protection of corporate information, corporate information space, corporate information protection policy.